Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт управления бизнес-процессами и экономики
Кафедра экономики и информационных технологий менеджмента

УТВЕРЖДАЮ
Заведующий кафедрой
_____ А.А. Ступина
подпись
«____» _____ 2017 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Консолидированная модель оценки эффективности использования виртуальных и облачных технологий

направление подготовки 09.04.03 «Прикладная информатика»

профиль подготовки 09.04.03.00.02 «Реинжиниринг бизнес-процессов»

Научный руководитель _____ профессор, д-р техн. наук А.А. Ступина
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник _____ Е.Е. Машинец
подпись, дата инициалы, фамилия

Рецензент _____ доцент, канд. техн. наук В.Ю. Журавлев
подпись, дата должность, ученая степень инициалы, фамилия

Красноярск 2017

РЕФЕРАТ

Актуальность работы заключается в том, что в последние годы в ИТ-сообществе широко распространилось мнение о том, что современные облачные технологии способны существенно сократить расходы, и сегодня многие компании все чаще переносят свои корпоративные системы и бизнес-приложения в облако. Об этом свидетельствуют результаты второго ежегодного исследования CiscoCloudWatch.

Целью данной магистерской диссертации является повышение уровня эффективности оценки ИТ-инфраструктуры организации с помощью консолидированной модели оценки эффективности использования виртуальных и облачных технологий.

Для достижения поставленной цели определены следующие задачи:

1. Провести анализ текущего состояния облачных технологий.
2. Изучить плюсы и минусы работы с облачными технологиями.
3. Проанализировать существующие методики оценки эффективности ИТ-проектов.
4. Разработать Консолидированную модель оценки эффективности использования виртуальных и облачных технологий.
5. Изучить и выбрать критерии оценки эффективности и рисков облачных технологий.

Научная новизна и теоретическая значимость диссертационной работы определяются разработкой новой модели и методов.

Общий объем работы – 76 страниц. Магистерская диссертация включает 5 таблиц, 36 рисунков. Список использованной литературы включает в себя 50 источников.

ABSTRACT

The urgency of the work lies in the fact that in recent years the IT community has widely spread the view that modern cloud technologies can significantly reduce costs, and today many companies are increasingly moving their corporate systems and business applications to the cloud. This is evidenced by the results of the second annual study of CiscoCloudWatch.

The purpose of this master's thesis is to improve the effectiveness of assessing the organization's IT infrastructure using a consolidated model for assessing the effectiveness of using virtual and cloud technologies.

To achieve this goal, the following tasks are defined:

1. Conduct an analysis of the current state of cloud technologies.

2. Explore the pros and cons of working with cloud technologies.

3. Analyze existing methods for assessing the effectiveness of IT projects.

4. Develop a Consolidated model for assessing the effectiveness of the use of virtual and cloud technologies.

5. To study and choose criteria of an estimation of efficiency and risks of cloud technologies.

The scientific novelty and theoretical significance of the dissertation work are determined by the development of a new model and methods.

The total amount of work is 76 pages. Master's thesis includes 5 tables, 36 drawings. The list of references includes 50 sources.

СОДЕРЖАНИЕ

Введение **5**

1 Анализ текущего состояния облачных технологий **9**

1.1 Общая характеристика облачных и виртуальных технологий 9

1.2 Облачные технологии в оптимизации бизнес-процессов компании 12

1.3 Проблемы и перспективы развития облачных технологий в России 17

2 Постановка задачи проектирования ИС **21**

2.1 Анализ путей решения имеющихся проблем 21

2.2 Определение цели и задач проектирования ИС 21

2.3 Выбор и обоснование проектных решений 23

2.3.1 Обоснование выбора технологии проектирования 23

2.3.2 Обоснование выбора среды разработки модели 23

2.4 Анализ методик для оценки рисков от внедрения ИТ-проектов 24

2.5 Концепция информационной системы 36

2.5.1 Построение диаграммы прецедентов 36

2.5.2 Построение каскадной модели последовательности работ 37

2.5.3 Документирование прецедентов 38

3 Проектирование консолидированной модели **40**

3.1 Функциональное обеспечение 40

3.1.1 Функциональная модель «как должно быть» 40

3.1.2 Функциональная архитектура 41

3.2 Технологическое обеспечение 44

3.2.1 Диаграмма контекста системы 44

3.2.2 Диаграмма сообщений 44

3.3 Информационное обеспечение 47

3.3.1 Построение диаграммы сущностных классов 47

3.3.1 Обоснование выбора метода экспертной оценки 47

3.3.3 Характеристика критериев оценки рисков 53

3.4 Аппаратное обеспечение 57

3.5 Руководство пользователя 57

3.6 Оценка эффективности ИТ-проекта 61

Заключение **69**

Список используемых источников **71**

Введение

Анализ эффективности и оценка рисков – ключевой фактор для успешного внедрения любой ИТ-инфраструктуры на предприятии.

Развитие научно-технического прогресса обусловило широкое внедрение информационных технологий (ИТ) во все области жизнедеятельности общества. ИТ позволили значительно упростить сбор и обработку разнообразных статистических данных о деятельности организации. Однако программное обеспечение для автоматизации управленческих процессов имеет очень большую стоимость. Внедрение таких решений может занимать длительное время, от месяцев до нескольких лет.

В современном ИТ-мире приобрели популярность облачные технологии (ИТ-сервисы), которые находятся еще в стадии становления для России. Облачные вычисления обладают огромными преимуществами по сравнению с обычными ИТ, но и риски более высоки.

В связи с этим, каждый ответственный руководитель не будет заниматься проектом внедрения проектов в области ИТ без предварительного расчета выгод от его эксплуатации, а это невозможно сделать без тщательного анализа и определения экономической необходимости, целесообразности и эффективности. Обязательной составляющей технико-экономического обоснования ИТ-проекта является оценка его экономической эффективности. Поэтому особую важность приобретают вопросы по выбору методики по оценке эффективности и рисков от внедрения ИТ.

Целью данной магистерской диссертации является повышение уровня эффективности оценки ИТ-инфраструктуры организации с помощью консолидированной модели оценки эффективности использования виртуальных и облачных технологий.

Назначение работы – разработать модель оценки эффективности оценки использования виртуальных и облачных технологий для организаций с предоставлением оценок рисков и внедрения защитных мер по их предотвращению в денежном эквиваленте.

Для достижения поставленной цели определены следующие задачи:

1. Провести анализ текущего состояния облачных технологий.
2. Изучить плюсы и минусы работы с облачными технологиями.
3. Проанализировать существующие методики оценки эффективности ИТ-проектов.
4. Разработать Консолидированную модель оценки эффективности использования виртуальных и облачных технологий.
5. Изучить и выбрать критерии оценки эффективности и рисков облачных технологий.

Объектом исследования является уровень оценки эффективности ИТ-проектов организации.

Предмет исследования – система оценки эффективности ИТ-проектов в организации.

Практическая значимость работы заключается в возможности применения консолидированной модели оценки эффективности использования виртуальных и облачных технологий организациями для улучшения оценки состояния ИТ-инфраструктуры.

Методы исследования. В соответствии с характером решаемых проблем в работе использовались методы оценки эффективности с помощью коэффициента ROI, а так же математического ожидания потерь.

Научная новизна и теоретическая значимость диссертационной работы определяются разработкой новой модели и методов:

1. Впервые предложена консолидированная модель оценки эффективности использования виртуальных и облачных технологий, которая отличается от моделей, применяемых для оценки эффективности традиционных ИТ-проектов, механизмом оценки рисков, возникающих при использовании облачных технологий с помощью математического ожидания потерь, экономического показателя ROI, а так же возможностью оценки вложений в систему защиты по предотвращению рисков.

2. Впервые предложено решение задачи оценки рисков на этапах оценки эффективности внедрения облачных технологий для дальнейшего успешного развития организации. Данная модель расчета позволяет научно обосновывать возможность и целесообразность использования облачных технологий с учетом рисков, влияющих на безопасность и удобство работы с данными ИТ-технологиями.

Актуальность работы заключается в том, что в последние годы в ИТ-сообществе широко распространилось мнение о том, что современные облачные технологии способны существенно сократить расходы, и сегодня многие компании все чаще переносят свои корпоративные системы и бизнес-приложения в облако. Об этом свидетельствуют результаты второго ежегодного исследования CiscoCloudWatch.

Согласно проведенным опросам, 90% руководителей IT-служб признают актуальность облачных технологий (ранее так считали 52% респондентов). 31% опрошенных специалистов считают сетевое облако критически важным фактором, влияющим на многое из того, чем занимается их компания. 85% организаций, где облачные решения "стоят на повестке дня", планируют в течение ближайшего года новые инвестиции в эту технологию.

Наиболее высоко стратегическую важность облачных вычислений оценивают предприятия розничной торговли и операторы связи (39 и 38 процентов, соответственно). В отличие от них, организации общественного сектора относятся к этой технологии намного более сдержанно: ее значимость признают лишь 24% государственных организаций и 18% учреждений здравоохранения.

В опубликованном CiscoSystems отчете отмечается, что главными препятствиями на пути распространения облачных технологий по-прежнему остаются опасения по поводу информационной безопасности и защиты конфиденциальных данных, хотя острота этих проблем снизилась: сегодня такую озабоченность выражают 52 процента опрошенных (для сравнения: в прошлых периодах данный показатель составлял 72 процента). Это означает,

что прогнозирование результатов использования будущих облачных технологий наиболее актуальна для руководителей организаций.

В первой части магистерской работы рассматривается предметная область и подробно изучаются проблемные места при работе с облачными технологиями. Проводится тщательное исследование бизнес-процессов облачных технологий, в результате чего выявляются достоинства и недостатки, на основании которых формируется экономическая сущность задачи.

Во второй части на основании информации о выявленных проблемах, ставятся задачи проектирования, и обосновывается применение методов их решения. При принятии решения о разработке системы рассматривается рынок готовых программных средств, способных обеспечить решение поставленных задач, а также, осуществляется выбор и обоснование проектных решений.

В третьей части магистерской работы разрабатывается консолидированная модель оценки эффективности использования виртуальных и облачных технологий, так же предоставляется реализация данной модели, на основании которой решаются проблемы, изложенные в аналитической части. В проектной части проектируются диаграммы сообщений, сущностных классов, приводится спецификация поведения задач и спецификация интерфейса класса, а так же руководство пользователя.

1 Анализ текущего состояния облачных технологий

1.1 Общая характеристика облачных и виртуальных технологий

Облачные вычисления (англ. cloudcomputing) – информационно-технологическая концепция, подразумевающая обеспечение повсеместного и удобного сетевого доступа по требованию к общему набору конфигурируемых вычислительных ресурсов (например, сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам – как вместе, так и по отдельности), которые могут быть оперативно предоставлены и высвобождены с минимальными эксплуатационными затратами или обращениями к провайдеру [12].

Особенностью облачных технологий является не привязанность к аппаратной платформе и географической территории, а возможность масштабируемости. Клиент может работать с облачными сервисами с любой точки планеты и с любого устройства имеющего доступ в интернет, а также оперативно реагировать на изменяющиеся бизнес-задачи компании и потребности рынка.

Концепция «Облачный хостинг» включает в себя следующие принципы:

1. “On-demandself-service” – принцип подразумевающий доступность услуг в любом объеме. Пользователь может купить любой интересующий его объем услуг по принципу “rentingtakesminutes”, т.е. всего за несколько минут.
2. “Ubiquitousnetworkaccess” – принцип доступности облачных решений с любых устройств: стационарного компьютера, ноутбука, планшета, мобильного телефона, коммуникатора и т.д.
3. “Metereduse” – услуги облачного хостинга оплачиваются по факту объема их использования за определенный промежуток времени. Оплачивается лишь объем использованных услуг.
4. “Elasticity” – принцип «гибкой» покупки. У пользователя есть возможность заказать малый объем услуг и пользоваться им в течение долгого времени или напротив, заказать большой объем услуг и потратить его за минимальный промежуток времени.

5. “Resourcepooling” – принцип независимости от аппаратной платформы. Конечный пользователь не знает, да и ему в принципе неважно, ресурсы какого аппаратного узла используют его виртуальные машины, либо на какой аппаратной платформе выполняются его приложения. Данная концепция позволяет не прекращать обслуживание пользователей при выходе из строя одного или нескольких аппаратных узлов, то есть облачный продукт не зависит от работоспособности одного отдельно взятого сервера [27].

VPS (англ. Virtual Private Server) или VDS (англ. VirtualDedicatedServer) Виртуальный сервер – услуга, в рамках которой пользователю предоставляется так называемый Виртуальный выделенный сервер. В плане управления операционной системой по большей части она соответствует физическому выделенному серверу. В частности: root-доступ, собственные IP-адреса, порты, правила фильтрования и таблицы маршрутизации.

Внутри виртуального сервера можно создавать собственные версии системных библиотек или изменять существующие, владелец сервера может удалять, добавлять, изменять любые файлы, включая файлы в корневой и других служебных директориях, а также устанавливать собственные приложения или настраивать/изменять любое доступное ему прикладное программное обеспечение.

В некоторых системах аппаратной виртуализации также доступны для редактирования настройки ядра операционной системы и драйверов устройств.

Виртуальный выделенный сервер эмулирует работу отдельного физического сервера. На одной машине может быть запущено множество виртуальных серверов. Помимо некоторых очевидных ограничений, каждый виртуальный сервер предоставляет полный и независимый контроль и управление, как предоставляет его обычный выделенный сервер.

Каждый виртуальный сервер имеет свои процессы, ресурсы, конфигурацию и отдельное администрирование. Обычно, в качестве виртуального сервера используются свободно распространяемые версии

операционных систем UNIX и Linux. Для эмуляции обычно используются технологии виртуальных машин.

Администратор (владелец) виртуального сервера может устанавливать любые приложения, работать с файлами и выполнять любые другие задачи, возможные на отдельной машине. Аренда виртуального сервера – популярный вид хостинга, так как предоставляет разумный баланс между ценой и возможностями для большинства владельцев интернет сайтов и приложений. Цена может сильно различаться в зависимости от пакета услуг поддержки и администрирования.

Виртуальные серверы без поддержки (unmanaged) предоставляются по низким (от нескольких долларов в месяц) ценам. Создание сайта на таком сервере может потребовать от владельца довольно обширных знаний по администрированию операционной системы и интернет приложений. Неподдерживаемый хостинг хорошо подходит для специалистов и энтузиастов.

Поддерживаемые (managed) виртуальные серверы варьируются в широких пределах и подходят тем, кто заинтересован направить все усилия на развитие сайта, а не на технические детали его содержания.

Любой интернет-хостинг относится к одному из следующих видов: виртуальный хостинг, VPS-хостинг, выделенный сервер и недавно появившийся облачный хостинг. Давайте рассмотрим, чем облачный тип хостинга отличаются от других типов.

VPS хостинг считается самым доступным по цене. Кроме того, стоит отметить, что виртуальный хостинг отличается небольшим функционалом и не может выдержать большого трафика. Облачный хостинг в отличие от виртуального характеризуется возможностью динамического распределения ресурсов физического сервера, что обеспечивает стабильную работу сайтов практически при любой посещаемости. Однако стоимость облачного хостинга выше, нежели, виртуального.

VPS в отличие от облачного хостинга представляет собой виртуальный выделенный сервер, что позволяет устанавливать необходимое ПО, а также не

зависеть от ресурсоемкости соседних хостингов. Но так как степень нагрузки на сервер варьируется по времени, то определенную часть суток ресурсы такого сервера будут попросту простаивать. Облачный же хостинг отличается почасовой тарификацией, причем тариф можно менять либо в ручном, либо в автоматическом режиме. Если ваш сайт посещается пока что слабо, можно взять самый дешевый тарифный план, если же счетчики посещаемости зашкаливают, можно арендовать целый кластер серверов.

Выделенный хостинг располагается на отдельном физическом сервере и до недавнего времени представлял наиболее мощную платформу.

Таким образом, характеристики облачного хостинга по большому количеству критериев опережают традиционные виды хостинга.

1.2 Облачные технологии в оптимизации бизнес-процессов компании

Хранение информации в облаке при наличии выхода в Интернет дает гарантию доступа к ней из любой точки планеты практически с любого устройства. Удобство облачных технологий уже успели по достоинству оценить пользователи крупных почтовых сервисов – gmail.com, mail.ru, yandex.ru. Облачные технологии можно легко настроить под потребности пользователя, приобретая дополнительное пространство для хранения информации или, напротив, отказываясь от лишнего. Работа с облачными технологиями позволяет мгновенно реагировать на появление новых бизнес-задач, снижает расходы и повышает эффективность компаний и их подразделений.

Такой подход к работе с информацией может быть рекомендован как индивидуальным предпринимателям и малому бизнесу, так и среднему и крупному бизнесу: для любого масштаба найдется эффективная бизнес-модель. Небольшие компании в первую очередь интересуются сервисами бухгалтерии и почты, приложениями для обмена информацией, восстановления и архивации информации. Более крупным организациям интересны виртуальные серверы и услуги связи, а также комплекс различных сервисов. Стартапы в сфере ИТ

используют облачные технологии, дающие им возможность обслуживать большое количество заказчиков, не вкладываясь в покупку дорого информационного оборудования [6].

Применяемые средства защиты облачных технологий обеспечивают на сегодняшний день высокий уровень безопасности информации. По данным Федеральной службы государственной статистики, 30,7% граждан, которые пользовались в 2013 г. государственными и муниципальными услугами, получали их в электронном виде. Для нужд Электронного Правительства внутри страны была спроектирована масштабная облачная инфраструктура.

Большое количество преимуществ говорит о том, что стоит рассмотреть возможность применения облачных технологий для бизнеса компании:

- использование интернет-сервисов без необходимости покупки серверов, сетевого оборудования, кондиционеров, лицензированного ПО;
- не требуется штатный IT-специалист, все это сокращает расходы на работу с информацией до 70%;
- подключение к облачным сервисам может быть произведено с любого мобильного устройства, имеющего выход в Интернет, и для этого не требуется специальных знаний в области IT;
- данные централизованы, что более удобно, чем информация, распределенная по разным филиалам и компьютерам;
- изменение объема облачного сервиса может быть реализовано специалистами компании-провайдера по запросу компании в течение нескольких минут;
- есть возможность самостоятельно управлять объемом облака через личный кабинет на сайте оператора;
- облачные сервисы проектируются с повышенной безопасностью и отказоустойчивостью и обеспечиваются техподдержкой круглосуточно [16].

Безопасность облачных технологий и решений подтверждена при помощи сертификации Федеральной службы по техническому и экспортному контролю

(ФСТЭК) России. Для получения сертификата программные продукты должны быть признаны соответствующими следующим нормативам:

1. Требования к системам обнаружения вторжений (ФСТЭК России, 2011).

2. Требования к средствам антивирусной защиты (ФСТЭК России, 2012).

3. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (Гостехкомиссия России, 1997).

4. Кроме того, следует обращать внимание на сертификацию центров обработки данных по TIER. Это международный сертификат, присваивающий дата-центрам классы надежности от I до IV. Лучшими по соотношению «цена-бесперебойность» являются дата-центры III класса [10].

Принцип работы

Облачная IT-инфраструктура для бизнеса базируется в дата-центрах, которые для повышения безопасности ранее очень часто располагались за рубежом. Отбор сотрудников в штат центра обработки данных проводится так же тщательно, как в банковские структуры. Клиентская информация хранится на защищенных от несанкционированного доступа высоконадежных носителях. Важные данные в случае ошибки клиентов могут быть восстановлены за счет специальной системы резервного копирования. Уровень защиты персональной и конфиденциальной информации таков, что многие провайдеры облачных услуг не всегда знают, какие приложения размещают в облаке клиента.

Практически любой облачный сервис можно запустить в срок от нескольких часов до пары дней. Для этого требуется оформить заявку на сайте компании-провайдера и внести предоплату. После поступления денег клиенту предоставляется доступ к сервисам классов IaaS (Infrastructure-as-a-Service), SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service).

«Виртуальные» решения для бизнеса

Наибольшую популярность в настоящее время приобрели следующие модели облачных технологий:

Аренда виртуального сервера (облачный центр обработки данных). Дата-центр, построенный на облачных технологиях, представляет собой серверы, диски и сети, доступные через Интернет или выделенные каналы связи. Для клиента создается портал самообслуживания, через который он сможет осуществлять управление данными. Это позволяет полностью контролировать все размещенные в облаке возможности независимо от провайдера услуг.

Виртуальный офис. Рабочее место можно организовать, не привязывая его к определенному компьютеру, – в виртуальном пространстве. В облаке воспроизводится внутренняя сеть компании, включая сетевые диски, общие папки, программы-планировщики. Виртуальный офис позволяет полноценно заменить стационарные рабочие компьютеры везде, где есть Интернет.

Резервное копирование. Возможность для частного виртуального дата-центра, предусмотренная для того, чтобы обеспечить сохранность данных в чрезвычайных случаях. Система резервного копирования гибко настраивается под текущий объем информации, что позволяет сократить временные и финансовые издержки

Катастрофоустойчивость (DRaaS). Сервис индивидуальных решений по обеспечению катастрофоустойчивости объединяет несколько облачных площадок с выходом на нескольких операторов связи. Безопасность данных достигается путем перекрестного резервного копирования в автоматизированном или ручном формате.

Гибридное облако. Это возможность подключить частное облако к публичной облачной структуре провайдера, чтобы разгрузить собственные мощности в период высокой деловой активности – например, при сдаче важных отчетов. Все некритичные на данный момент процессы переносятся в облако провайдера, а потом возвращаются обратно. Это позволяет существенно ускорить процессы в собственном облаке.

Аренда приложений. Программное обеспечение можно не покупать для установки на компьютер, а получать через Интернет, оплатив пользование на нужный срок. При этом клиенту гарантируется круглосуточная техническая поддержка и безопасность данных

Виртуальный контакт-центр Организация традиционного контакт-центра требует специального помещения, оборудования рабочих мест и оплаты труда офисных работников. Виртуальный контакт-центр, организованный по облачной технологии, позволяет высвободить огромное количество ресурсов и развернуть работу за два дня с момента подачи заявки провайдеру.

Частное облако. Это виртуальная инфраструктура, созданная для нескольких подразделений одной компании, ее клиентов и подрядчиков. Частное облако может являться шлюзом к общедоступному облаку, одновременно обеспечивая использование постоянно растущего набора услуг и сохраняя важные для конкретного бизнеса информационные системы внутри.

Развитие облачных технологий в будущем

Делать ставку на облачные информационные технологии, не представляя себе их перспектив, было бы несерьезно.

Уже известно, что бизнес облачных технологий является одним из самых бурно развивающихся в ИТ-сфере. Это автоматически означает уменьшение стоимости данных услуг и совершенствовании технического и программного обеспечения в ближайшем будущем. Безопасность и эффективность облачных технологий стали практически общепризнанными, уже идет проработка юридических аспектов работы облачных систем и создание новых экономических моделей использования ИТ-услуг [26].

В мировой практике тенденция к переходу бизнеса на облачные технологии уже сложилась. Этот вопрос, по данным компании Symantec, обсуждается в 90% компаний. Многие российские компании в погоне за стопроцентным контролем над информацией (как они сами полагают) стремятся держать ценные ресурсы строго при себе. Однако практика показывает, что инфраструктура облака стабильнее и безопаснее по сравнению

с инфраструктурами клиентов. Это объясняется более высокими затратами и уровнем знаний, которые требуются для создания надежных дата-центров. Не каждая крупная компания располагает подобными возможностями[3].

1.3 Проблемы и перспективы развития облачных технологий в России

В современных условиях эффективность и успешность бизнеса в значительной степени зависит от скорости, с которой он реагирует на изменения ситуации на рынке. Этот фактор в сочетании с производительностью становится стратегическим активом компаний различных отраслей экономики. Применение передовых информационных технологий все чаще становится решающим фактором успеха, главным критерием в борьбе за лидерство. Внедрение облачных сервисов в российский малый и средний бизнес позволит не только модернизировать его деятельность, но и повысить конкурентоспособность с иностранными компаниями. Что в условиях вступления в ВТО является актуальной задачей.

Российский рынок облачных технологий стартовал относительно недавно – в 2005-2006 годах. Потому Россия в мировом рейтинге – еще занимает достаточно малую долю рынка. При этом аналитики прогнозируют на ближайшие года – исключительно позитивный рост данного рынка.

В российской предпринимательской практике на аутсорсинг чаще всего передаются такие функции, как ведение бухгалтерского учёта, обеспечение функционирования офиса, переводческие услуги, поддержка работы компьютерной сети и информационной инфраструктуры, рекламные услуги, обеспечение безопасности.

Перед большой частью клиентов, компаний малого и среднего бизнеса, активно развивающихся и быстро растущих, сегодня стоит задача управления своим ростом. Руководители осознают, что им крайне необходима корпоративная почта и свой сайт, общие календари и справочник сотрудников, и доступ ко всему этому должен быть с любого мобильного устройства в любой

точке мира. Но у руководителей нет времени и денег думать над IT-ресурсами самим. Так на помощь им приходят облачные технологии [20].

Данные достоинства экономически выгодны для предприятий, так как позволяют сократить затраты, высвободить денежные средства для использования их в других сферах деятельности. Основные преимущества данной технологии заключаются в следующем для внедрения в компанию:

1. Доступность – облачные технологии доступны всем, из любой точки, где есть интернет, с любого компьютера, где есть браузер.
2. Низкая стоимость – основные факторы снизившие стоимость использования облаков следующие:
   - снижение расходов на обслуживания виртуальной инфраструктуры;
   - оплата фактического использования ресурсов.
3. Гибкость – неограниченность вычислительных ресурсов (память, процессор, диски), за счет использования систем виртуализации, процесс масштабирования.
4. Надежность – надежность облачных технологий, особенно находящихся в специально оборудованных центрах обработки данных.
5. Безопасность.
6. Быстрое внедрение, так как не нужно не ждать пока установят все необходимое оборудование и ПО на компьютеры предприятия.

К сожалению, как и все технологии эта тоже несовершенна. У нее тоже есть ряд недостатков – это:

1. Необходимость постоянного стабильного соединения с сетью.
2. Программное обеспечение – есть ограничения по ПО, которое можно разворачивать на облачных технологиях и предоставлять его пользователю.
3. Конфиденциальность – конфиденциальность данных хранимых на публичных облачных технологиях в настоящее время вызывает много споров, но в большинстве случаев эксперты сходятся на том, что не рекомендуется хранить наиболее ценные для компании документы на публичном облаке так

как в настоящее время нет технологии, которая бы гарантировала 100% конфиденциальность хранимых данных.

4. Невозможность восстановления информации находящейся в облаке.

5. И прочие проблемы, которые в ближайшей перспективе, скорее всего, будут устранены либо сведены к минимуму [7].

Помимо недостатков присущих самой технологии существует ряд причин, которые мешают развитию облачных технологий на российском рынке. Их можно поделить на две логические группы: объективные и субъективные. К первой категории относятся два фактора: недостаточное развитие услуг широкополосного доступа в интернет из данной проблемы вытекает еще одна, взаимосвязанная с ней, это недостаточно развитая инфраструктура связывающая центр и регионы. Другой фактор – законодательство. Несмотря на то, что об облачных технологиях говорят уже не первый год, правовое поле, в рамках которого могут быть урегулированы спорные ситуации, отсутствует.

К субъективным причинам можно отнести следующие:

- уязвимость в области информационной безопасности. Опасения небезосновательны;
- недостаточная зрелость бизнес-процессов ИТ- и телеком-провайдеров, в итоге внедрение облачных технологий может оказаться дороже строительства собственной инфраструктуры или покупки коробочных решений;
- ограниченность в доработке и интеграции приложений, действительно, сегодня большим вопросом остается, например, возможность интеграции существующей инфраструктуры и «облачных» вычислений, совместимость облачных технологий различных провайдеров;
- отсутствие доверия к компаниям, предоставляющих сервисы, для появления его компаниям необходимо показать, что они способны поддерживать тот уровень конфиденциальности, целостности и доступности данных, который обеспечивают сам компании. Данное условие важно для

компаний, так как они отдают свою самую большую ценность - коммерческую тайну в чужие руки.

- отсутствие стандартизации услуг, на сегодня предложения поставщиков даже простейших сервисов практически не стандартизованы и трудно сравнимы, но именно из-за стандартизации появляется экономическая выгода для как поставщика облачных ИТ - сервисов, так и для потребителя, отсутствие стандартов затрудняет конкуренцию между провайдерами и не позволяет им активно развиваться, рынок таких услуг становится непрозрачным, а значит неминуемо более дорогим и другие.

Оценить все плюсы и минусы от использования облачных технологий – непростая задача, ведь неправильная оценка ИТ-проекта принесет немыслимые расходы организации. Поэтому руководителям организаций, планирующим переход в облако, необходимо иметь под рукой инструментарий оценки эффективности внедрения облачных и виртуальных технологий, позволяющий без особых усилий определить прогнозы будущего ИТ-проекта [2].

2 Постановка задачи проектирования ИС

2.1 Анализ путей решения имеющихся проблем

На основании анализа целей, задач и проблем предметной области были предложены стратегии решения проблем организации в таблице 1.

Таблица 1 – Стратегии решения проблем

Цель	Стратегия	Преимущества	Недостатки
Уменьшить работу Менеджера	1. Нанять еще одного специалиста	Сокращение времени на создание отчетов	Увеличение затрат на зарплату нового сотрудника; Увеличение трудовых ресурсов на создание отчетов
	2. Заказывать отчеты в другой фирме	Сокращение времени на создание отчетов	Постоянные затраты на оплату услуг другой фирмы; Возможны очереди в оказании услуг, что приведет к увеличению времени на создание отчетов
	3. Создание собственной Консолидированной модели оценки ИТ-проекта	Сокращение времени на создание отчетов; Возможное сокращение персонала	Временные затраты на разработку модели

Оптимальным вариантом решения проблемы было выбрано «Создание собственной Консолидированной модели оценки ИТ-проекта [8].

2.2 Определение цели и задач проектирования ИС

Под целью проектирования автоматизированных ИС подразумевается получение определённых значений экономического эффекта в сфере управления какими-либо процессами системы или снижение стоимостных и трудовых затрат на обработку информации, улучшение качества и достоверности получаемой информации, повышение оперативности её обработки и т.д., т.е. получение косвенного и прямого эффекта от внедрения данной задачи.

Целью проектирования данного проекта является разработка процесса оценки эффективности внедрения ИТ-проекта в организации.

Данная модель позволит сократить временные ресурсы и упростить оценку эффективности, а так же повысить качество оцениваемых показателей.

В рамках поставленных целей сформируем задачи в таблице 2, при выполнении которых, мы их достигнем.

Таблица 2 – Выбор задач

Подсистемы ВКР	Необходимо разработать
1. Функциональная архитектура предметной области	Да
2. Технологическое обеспечение (разработка технологии сбора, передачи, обработки и выдачи информации)	Да
3. Информационное обеспечение	
3.1. Разработка классификаторов и системы кодирования	Да
3.2. Разработка информационной модели (DFD)	Да
3.3. Разработка состава и содержания входных и выходных документов, метода их построения	Да
3.4. Разработка концептуальной и логической модели данных	Да
3.5. Разработка экранных и печатных форм входных и выходных документов	Нет
4. Математическое и алгоритмическое обеспечение	
4.1. Математические модели	Уже имеются
4.2. Алгоритмы решения задач	Нет
5. Программное обеспечение	
5.1. Инструкции по применению программ (руководство пользователя)	Да
5.2. Выбор системного программного обеспечения	Да

На основании анализа формулируются задачи проектирования:

- реорганизовать бизнес-процесс оценки эффективности ИТ-проектов;
- выполнить анализ имеющихся программ с оценкой применимости их к решению задач проекта;
- разработать консолидированную модель оценки эффективности использования виртуальных и облачных технологий;

- написать инструкции по использованию модели;
- разработать интуитивно понятный визуальный интерфейс.

2.3 Выбор и обоснование проектных решений

2.3.1 Обоснование выбора технологии проектирования

Выбор методов и средств проектирования, и разработки играет ключевую роль в задаче успешного достижения поставленных целей, поэтому необходимо точно определить какие из средств разработки следует использовать.

При проектировании будет использован следующий инструментарий: StarUML 2.0.

StarUML представляет собой программное средство UML-моделирования. Это гибкий, быстрый, многофункциональный, а также расширяемый инструмент UML.

Одной выдающейся особенностью StarUML является схема обзора, которая позволяет пользователю видеть текущее состояние проекта. Обладает возможностью выбора рисования: вручную, либо выбрать один из шаблонов и изменить его под свои потребности. Созданный проект можно экспортировать в формат JPEG или WMF.

StarUML предлагает широкий спектр функций и возможностей для создания схем баз данных с помощью UML-диаграмм. Легкость создания блок-схем или диаграмм – основное преимущество проекта StarUML[5].

2.3.2 Обоснование выбора среды разработки модели

Так как существующая модель оценки эффективности внедрения виртуальных и облачных сред на базе технологий EMC/VMware уже разработана в MicrosoftExcel, то рекомендуется реализовывать модель рисков так же MicrosoftExcel для удобства пользователя.

Данный табличный редактор является наиболее популярным среди организаций разного уровня и в связи с этим наша модель будет доступной для большинства пользователей.

2.4 Анализ методик для оценки рисков от внедрения ИТ-проектов

Для решения этой задачи были разработаны программные комплексы анализа и контроля информационных рисков: британский CRAMM (компания InsightConsulting), американский RiskWatch (компания RiskWatch) и российский ГРИФ (компания DigitalSecurity). Рассмотрим данные методы и построенные на их базе программные системы.

CRAMM

Метод CRAMM (the UK GovermentRiskAnalysisandManagmentMethod) был разработан Службой безопасности Великобритании (UK SecurityService) по заданию Британского правительства и взят на вооружение в качестве государственного стандарта. Он используется, начиная с 1985 года, правительственными и коммерческими организациями Великобритании. К настоящему моменту CRAMM приобрел популярность во всем мире. Фирма InsightConsultingLimited занимается разработкой и сопровождением программного продукта, реализующего метод CRAMM.

Метод CRAMM выбран для более детального рассмотрения и это не случайно. В настоящее время CRAMM – это довольно серьезный и универсальный инструмент, позволяющий, помимо анализа рисков, решать также и ряд других аудиторских задач, включая:

- проведение обследования ИС и выпуск сопроводительной документации на всех этапах обследования;
- проведение аудита в соответствии с требованиями Британского правительства, а также стандарта BS 7799:1995 – CodeofPracticeforInformationSecurityManagement BS7799;
- разработку политики безопасности и плана обеспечения неизменности бизнеса.

В основе CRAMM, в котором сочетаются количественные и качественные методы анализа, лежит комплексный подход к оценке рисков. Метод является многогранным и подходит как для больших, так и для мелких компаний, как государственного, так и коммерческого сектора. Версии программного обеспечения CRAMM, ориентированные на разные типы компаний, отличаются друг от друга своими базами знаний (profiles). Для коммерческих компаний имеется коммерческий профиль (CommercialProfile), для государственных компаний – правительственный профиль (Governmentprofile). Правительственный вариант профиля, также позволяет проводить аудит на соответствие требованиям американского стандарта ITSEC («Оранжевая книга»).

Использование метода CRAMM позволяет получать блестящие результаты, наиболее важным из которых, пожалуй, является возможность экономического обоснования расходов компании на обеспечение информационной безопасности и неизменности бизнеса. Экономически обоснованная политика управления рисками позволяет, в конечном итоге, экономить деньги, избегая неоправданных расходов.

CRAMM предполагает разделение всей процедуры на три последовательных этапа. Задачей первого этапа является ответ на вопрос: «Достаточно ли для защиты системы применения средств базового уровня, реализующих традиционные функции безопасности, или необходимо проведение более детального анализа?» На втором этапе производится распознавание рисков и оценивается их величина. На третьем этапе решается вопрос о выборе адекватных контрмер.

Методика CRAMM для каждого этапа определяет набор исходных данных, процедуру мероприятий, анкеты для проведения интервью, списки проверки и набор отчетных документов.

Если по результатам проведения первого этапа, установлено, что уровень критичности ресурсов является очень низким и существующие риски заведомо не превысят некоторого основного уровня, то к системе предъявляется

минимальный набор требований безопасности. В этом случае большая часть мероприятий второго этапа не выполняется, а осуществляется переход к третьему этапу, на котором формируется стандартный список контрмер для обеспечения соответствия основному набору требований безопасности.

На втором этапе производится анализ угроз безопасности и уязвимостей. Исходные данные для оценки угроз и уязвимостей аудитор получает от уполномоченных представителей компании в ходе соответствующих интервью. Для проведения интервью используются специализированные опросные листы (рисунок 1).

На третьем этапе решается задача управления рисками, состоящая в выборе адекватных контрмер. Решение о внедрении в систему новых механизмов безопасности и модификации старых принимает руководство компании, учитывая связанные с этим расходы, их приемлемость и конечную выгоду для компании. Задачей аудитора является обоснование рекомендуемых контрмер для руководства компании.

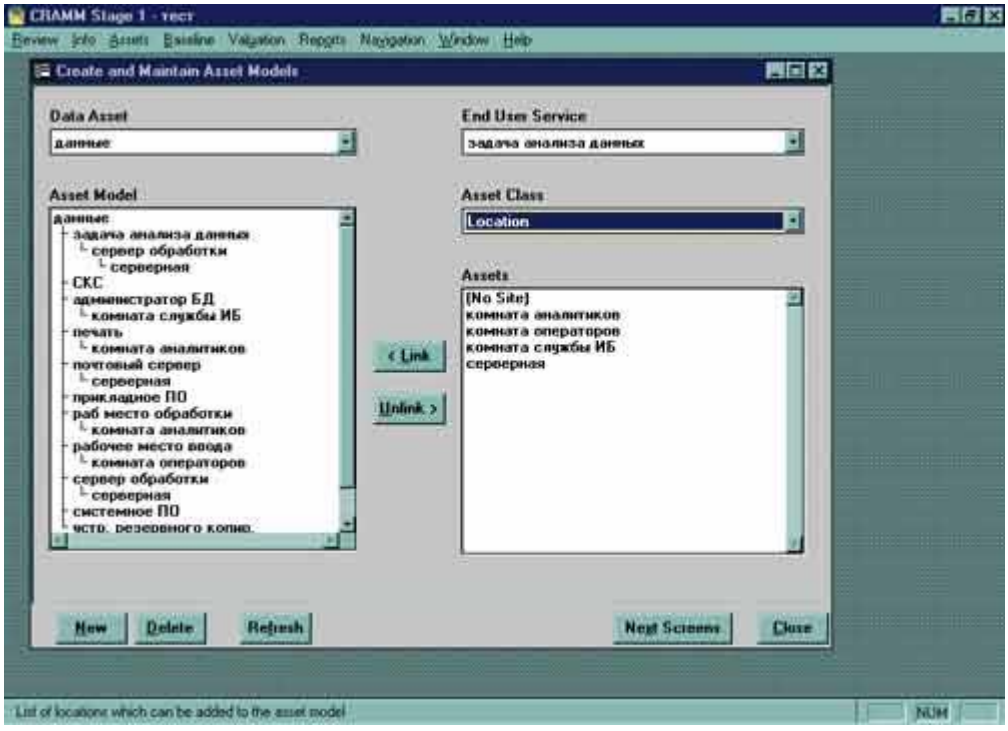


Рисунок 1 – Интерфейс риск-модели CRAMM

В случае принятия решения о внедрении новых контрмер и модификации старых, на аудитора может быть возложена задача подготовки плана внедрения

новых контрмер и оценки эффективности их использования. Решение этих задач выходит за рамки метода CRAMM.

Концептуальная схема проведения обследования по методу CRAMM показана на схеме 2.

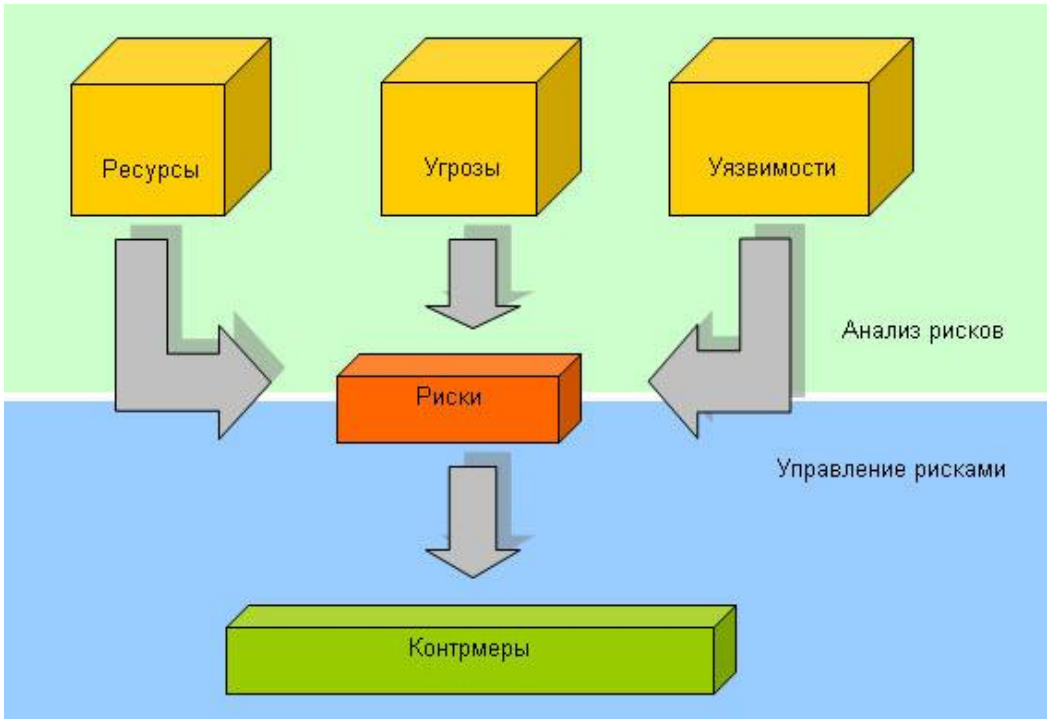


Рисунок 2 – Концептуальная схема обследования по методу CRAMM

К недостаткам метода CRAMM можно отнести следующее:

- использование метода CRAMM требует специальной подготовки и высокой квалификации аудитора;
- CRAMM в гораздо большей степени подходит для аудита уже существующих ИС, находящихся на стадии эксплуатации, нежели чем для ИС, находящихся на стадии разработки;
- аудит по методу CRAMM – процесс очень трудоемкий и может потребовать месяцев непрерывной работы аудитора;
- программный инструментарий CRAMM генерирует большое количество бумажной документации, которая не всегда оказывается полезной на практике;
- CRAMM не позволяет создавать собственные шаблоны отчетов или изменять имеющиеся;

- возможность внесения данных в базу знаний CRAMM недоступна пользователям, что вызывает трудности при адаптации этого метода к потребностям конкретной компании;
- ПО CRAMM существует только на английском языке;
- высокая стоимость лицензии.

RiskWatch

Программное обеспечение RiskWatch, разрабатываемое американской компанией RiskWatch, является мощным средством анализа и управления рисками. В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности. Оно включает в себя следующие средства аудита и анализа рисков:

- RiskWatchforPhysicalSecurity – для физических методов защиты ИС;
- RiskWatch for Information Systems – для информационных рисков;
- HIPAA-WATCH forHealthcareIndustry – для оценки соответствия требованиям стандарта HIPAA;
- RiskWatch RW17799 for ISO17799 – для оценки требованиям стандарта ISO17799.

В методе RiskWatch в качестве критериев для оценки и управления рисками используются предсказание годовых потерь (AnnualLossExpectancy – ALE) и оценка возврата от инвестиций (ReturnonInvestment – ROI). Семейство программных продуктов RiskWatch, имеет много достоинств.

RiskWatch помогает провести анализ рисков и сделать обоснованный выбор мер и средств защиты. Используемая в программе методика включает в себя 4 фазы:

Первая фаза – определение предмета исследования. На данном этапе описываются общие параметры компании – тип организации, состав исследуемой системы, базовые требования в области безопасности. Описание группируется в ряде подпунктов, которые можно выбрать для более подробного описания или пропустить.

Далее каждый из выбранных пунктов описывается подробно. Для облегчения работы аналитика в шаблонах даются списки категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты. Из них нужно выбрать те, что реально присутствуют в компании.

Вторая фаза – ввод данных, описывающих конкретные характеристики системы. Данные могут вводиться вручную или импортироваться из отчетов, созданных инструментальными средствами исследования уязвимости компьютерных сетей. На этом этапе подробно описываются ресурсы, потери и классы инцидентов.

Классы инцидентов получаются путем сопоставления данных потерь и данных ресурсов. Для выявления возможных уязвимостей используется опросный лист, база которого содержит более 600 вопросов, связанных с данными ресурсов. Допускается корректировка вопросов, исключение или добавление новых. Задается частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов. Все это используется в дальнейшем для расчета эффективности внедрения средств защиты.

Третья фаза – оценка рисков. Сначала устанавливаются связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих этапах. Для рисков рассчитываются математические ожидания потерь за год по формуле:

$$m=p * v, \quad (2)$$

где p – частота возникновения угрозы в течение года, v – стоимость ресурса, который подвергается угрозе.

Например, если стоимость сервера $150 000, а вероятность того, что он будет уничтожен пожаром в течение года, равна 0.01, то ожидаемые потери составят $1 500. Дополнительно рассматриваются сценарии что если..., которые позволяют описать аналогичные ситуации при условии внедрения средств защиты. Сравнивая ожидаемые потери при условии внедрения защитных мер и без них можно оценить эффект от таких мероприятий (рисунок 3).

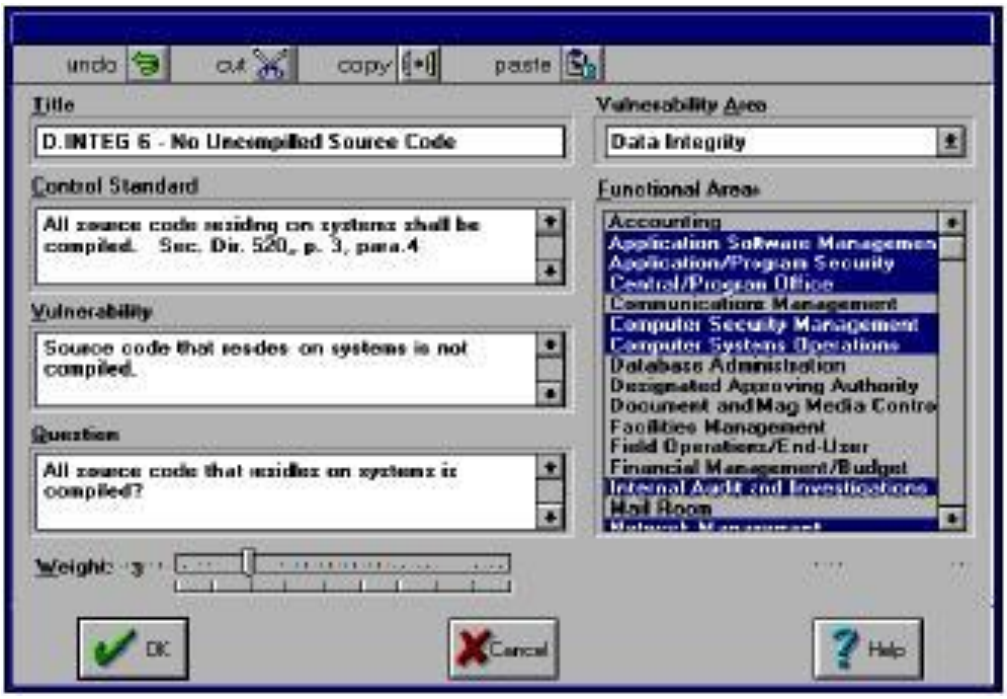


Рисунок 3 – Интерфейс риск-модели RiskWatch

Четвертая фаза – генерация отчетов. Типы отчетов: краткие итоги; полные и краткие отчеты об элементах, описанных на стадиях 1 и 2; отчет о стоимости защищаемых ресурсов и ожидаемых потерь от реализации угроз; отчет об угрозах и мерах противодействия; отчет о результатах аудита безопасности.

К недостаткам RiskWatch можно отнести:

- такой метод подходит, если требуется провести анализ рисков на программно-техническом уровне защиты, без учета организационных и административных факторов, полученные оценки рисков (математическое ожидание потерь) далеко не исчерпывают понимание риска с системных позиций – метод не учитывает комплексный подход к информационной безопасности;
- ПО RiskWatch существует только на английском языке;
- высокая стоимость лицензии – от $15 000 за одно рабочее место для небольшой компании и от $125 000 за корпоративную лицензию

ГРИФ

Для проведения полного анализа информационных рисков, прежде всего, необходимо построить полную модель информационной системы с точки

зрения информационной безопасности. Для решения этой задачи ГРИФ, в отличие от представленных на рынке западных систем анализа рисков, довольно громоздких и часто не предполагающих самостоятельного использования ИТ-менеджерами и системными администраторами, ответственными за обеспечение безопасности информационных систем компаний, обладает простым и очень понятным для пользователя интерфейсом. Однако за внешней простотой скрывается сложный алгоритм анализа рисков, учитывающий более ста параметров, который позволяет на выходе дать точную оценку существующих в информационной системе рисков, основанную на анализе особенностей практической реализации информационной системы.

Основная задача системы ГРИФ – дать возможность ИТ-менеджеру самостоятельно (без привлечения внешних экспертов) оценить уровень рисков в информационной системе и эффективность существующей практики по обеспечению безопасности компании, а также представить доказательства (в цифрах) для руководства компании о необходимости инвестиций в сферу ее информационной безопасности.

На первом этапе метода ГРИФ проводится опрос ИТ-менеджера с целью определения полного списка информационных ресурсов, представляющих важность для компании.

На втором этапе проводится опрос ИТ-менеджера с целью ввода в систему ГРИФ всех видов информации, представляющей важность для компании. Введенные группы важной информации должны быть размещены пользователем на указанных на предыдущем этапе объектах хранения информации (серверах, рабочих станциях и т. д.). Заключительная фаза – указание ущерба по каждой группе важной информации, расположенной на соответствующих ресурсах, по всем видам угроз (рисунок 4, 5).

На третьем этапе проходит определение всех видов пользовательских групп с указанием числа пользователей в каждой группе.

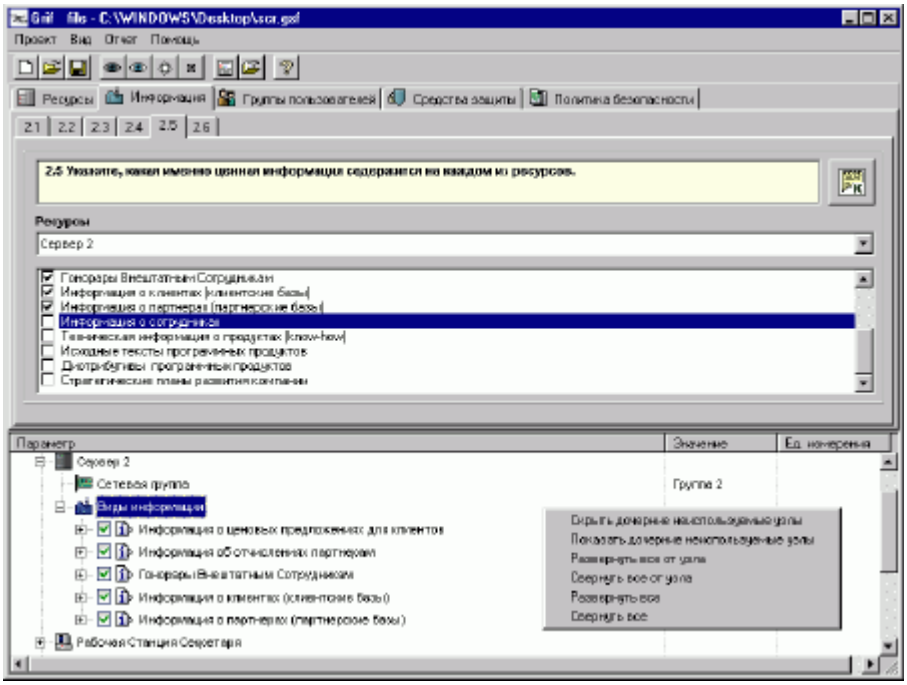


Рисунок 4 – Интерфейс риск-модели ГРИФ

Затем фиксируется, к каким группам информации на ресурсах имеет доступ каждая из групп пользователей. В заключение определяются виды (локальный и/или удаленный) и права (чтение, запись, удаление) доступа пользователей ко всем ресурсам, содержащим важную информацию.

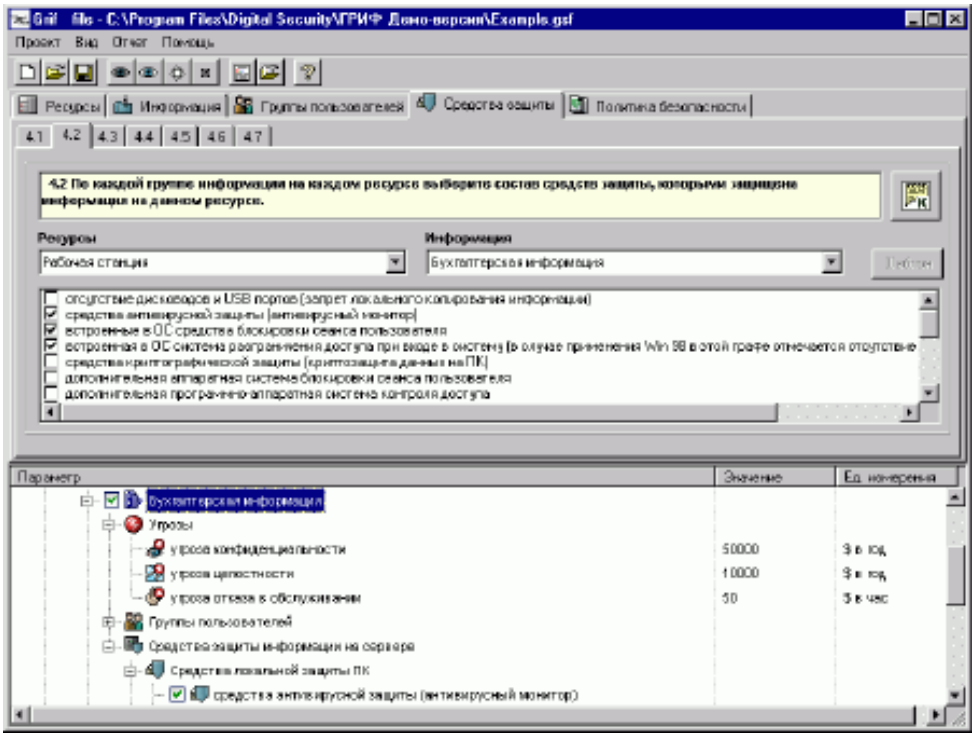


Рисунок 5 – Интерфейс риск-модели ГРИФ

На четвертом этапе проводится опрос ИТ-менеджера для определения средств защиты важной информации на ресурсах. Кроме того, в систему

вводится информация о разовых затратах на приобретение всех применяющихся средств защиты информации и ежегодные затраты на их техническую поддержку, а также ежегодные затраты на сопровождение системы информационной безопасности компании.

На завершающем этапе необходимо ответить на вопросы по политике безопасности, реализованной в системе, что позволит оценить реальный уровень защищенности системы и детализировать оценки рисков.

Наличие средств информационной защиты, отмеченных на первом этапе, само по себе еще не делает систему защищенной в случае их неадекватного использования и отсутствия комплексной политики безопасности, учитывающей все аспекты защиты информации, включая вопросы организации защиты, физической безопасности, безопасности персонала, непрерывности ведения бизнеса и т. д.

В результате выполнения всех действий по данным этапам, на выходе будет сформирована полная модель информационной системы с точки зрения информационной безопасности с учетом реального выполнения требований политики безопасности, что позволит перейти к программному анализу введенных данных для получения оценки рисков и формирования итогового отчета.

Подробный отчет по системе, дающий картину возможного ущерба, готов для представления руководству компании на рисунке 6.

К недостаткам ГРИФ можно отнести:

- отсутствие привязки к бизнес-процессам (запланировано в следующей версии);
- отсутствие возможности сравнения отчетов на разных этапах внедрения комплекса мер по обеспечению защищенности (запланировано в следующей версии);

отсутствие возможности добавления специфичных для данной компании требований политики безопасности.

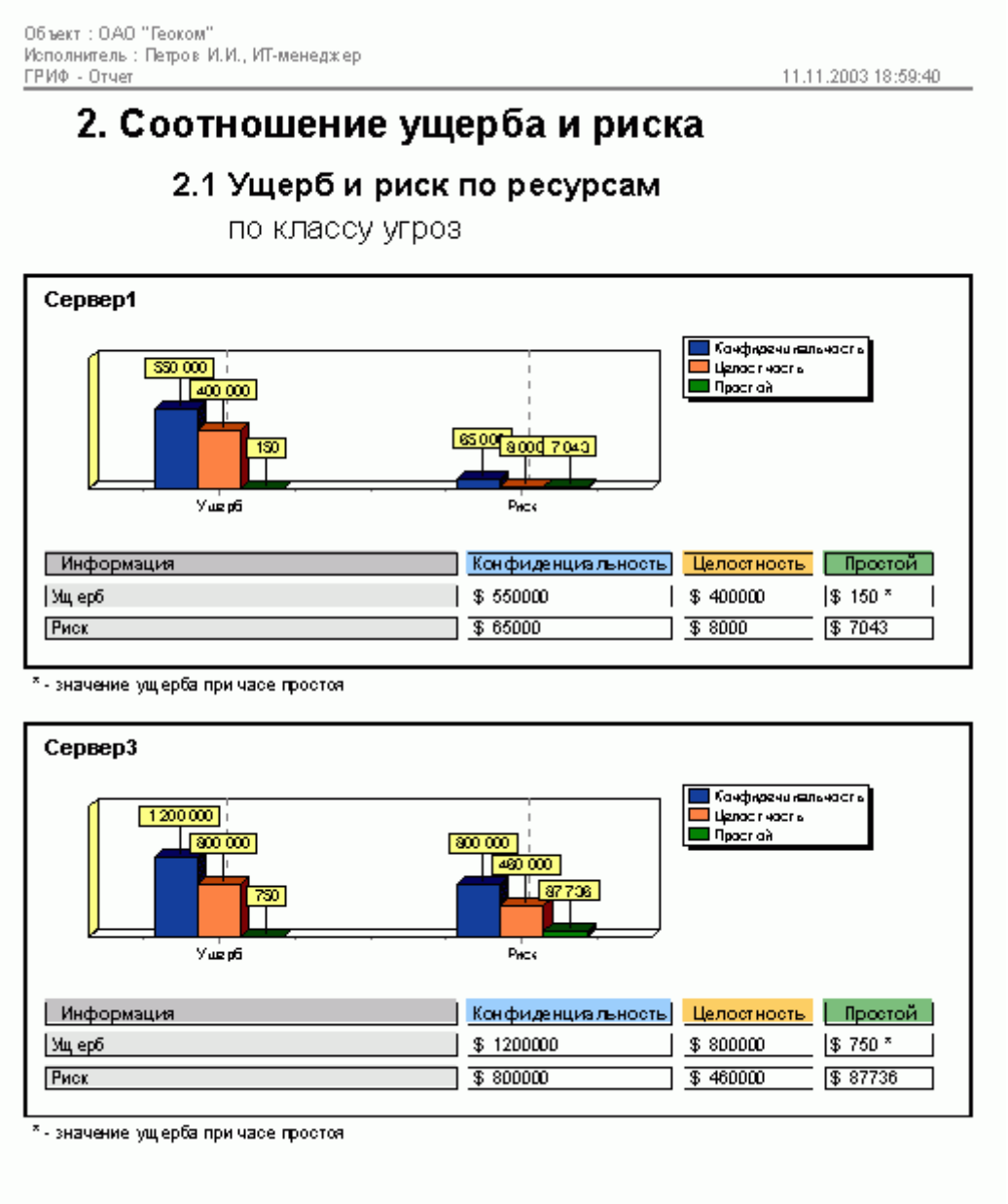


Рисунок 6 – Отчет «Соотношение ущерба и риска

Важно отметить, что ни одна из существующих моделей по оценке рисков информационных технологий полностью не подходит для случая облачных вычислений, т.к. ни в одной из них не учитываются специфика модели взаимодействия, присущая облачным средам. Эта специфика заключается в возможности удалённого доступа к предоставляемым сервисам.

Таблица 4 – Анализ моделей по оценке рисков информационных технологий

Критерии сравнения / Продукт	CRAMM, Central Computer and Telecommunications Agency (UK)	RiskWatch , Компания RiskWatch (USA)	ГРИФ Digital Security Office, Компания «Digital Security» (Россия)
Поддержка	Обеспечивается	Обеспечивается	Обеспечивается
Легкость в работе конечного пользователя	Использование метода CRAMM требует специальной подготовки и высокой квалификации аудитора.	Использование метода RiskWatch требует специальной подготовки и высокой квалификации аудитора.	Интерфейс программы ориентирован на ИТ-менеджеров и руководителей. Не требует специальных знаний в области информационной безопасности.
Цена	Стоимость лицензии от 2000 до 5000 долл. за одно рабочее место.	Стоимость лицензии от 10 000 долл. за одно рабочее место.	Стоимость лицензии от 1000 долл. за одно рабочее место.
Системные требования	Свободное дисковое пространство - 50 MB; Оперативная память - 64 MB; Операционная система - Windows.	Оперативная память - 256 MB RAM ; Свободное дисковое пространство - 30 Операционная система - Windows.	Оперативная память - 512 Mb. Свободное дисковое пространство - 1 Gb. Операционная система - Windows.
Наличие оценки минимизации рисков	Отсутствует	Отчет об угрозах и мерах противодействия	Выбранные контрмеры; Рекомендации экспертов.
Используемый метод оценивания рисков	Качественная оценка	Количественная оценка на основании математического ожидания потерь	Качественная оценка; количественная экспертная оценка значения риска для каждого ресурса
Наличие специального решения	Отсутствует	Отсутствует	Отсутствует

В связи с этим появляется необходимость рассматривать следующие возможные риски:

- юридические проблемы поставщика;
- эксплуатационные проблемы или простои поставщика;
- проблемы восстановления данных и конфиденциальности;

- общие проблемы безопасности;
- атаки на систему извне;
- проблемы отказа доступа к внешним каналам связи и внутренним.

Поэтому было принято решение о создании собственной модели оценки рисков с учетом перечисленных выше факторов [1].

Оценивание рисков мы будем проводить с помощью метода математического ожидания потерь за год, используемого в риск-модели RiskWatch, так как из всех выше перечисленных методов оценки рисков он наиболее наглядно поможет продемонстрировать изменение коэффициента возврата инвестиции ROI при внедрении облачных технологий [21].

2.5 Концепция информационной системы

2.5.1 Построение диаграммы прецедентов

Обобщив выбранные проектные решения, изложим видение будущей модели в виде концепции требований, используя метод проектирования StarUML на «Диаграмме прецедентов» укажем (Рисунок 7):

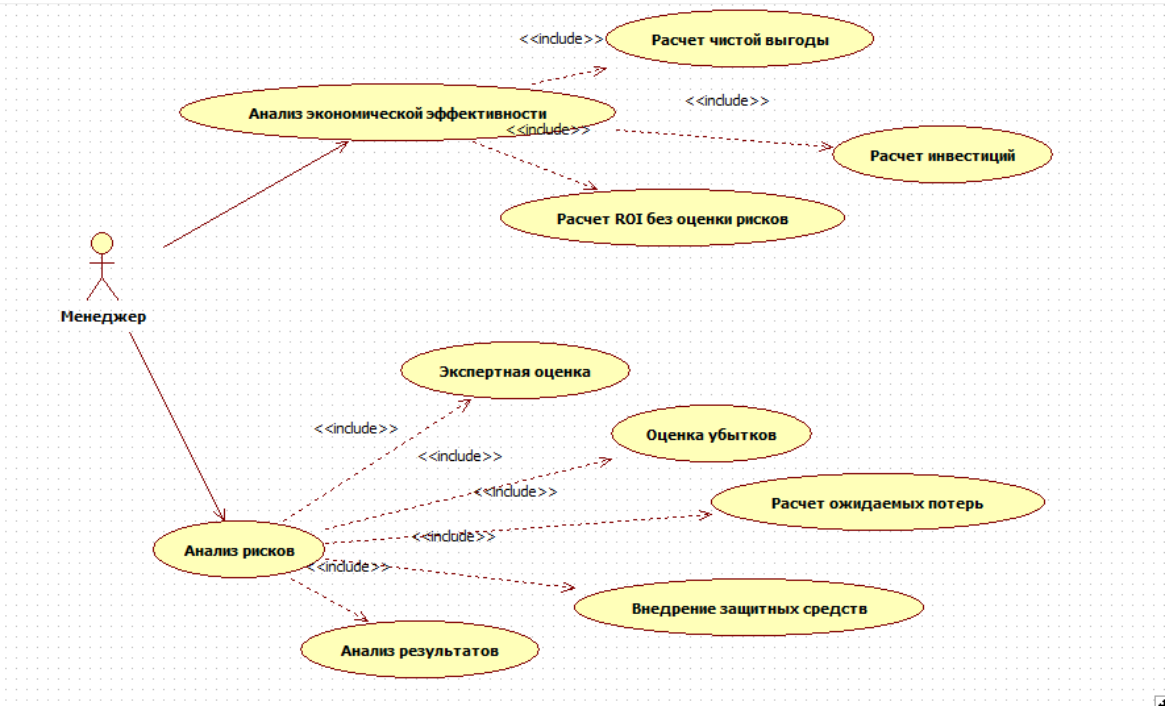


Рисунок 7 – Диаграмма прецедентов

- Актер – «Менеджер», который будет взаимодействовать с моделью;
- Прецеденты – «Анализ экономической эффективности» и «Анализ данных», устанавливающие последовательность взаимодействий между актером Менеджером и системой.

Ассоциативное отношение, показывающее, что актер Менеджер инициирует выполнение прецедентов «Анализ экономической эффективности» и «Анализ данных» [25].

2.5.2 Построение каскадной модели последовательности работ

Каскадная модель предусматривает последовательное выполнение всех этапов проекта в строго фиксированном порядке. Переход на следующий этап означает полное завершение работ на предыдущем этапе.

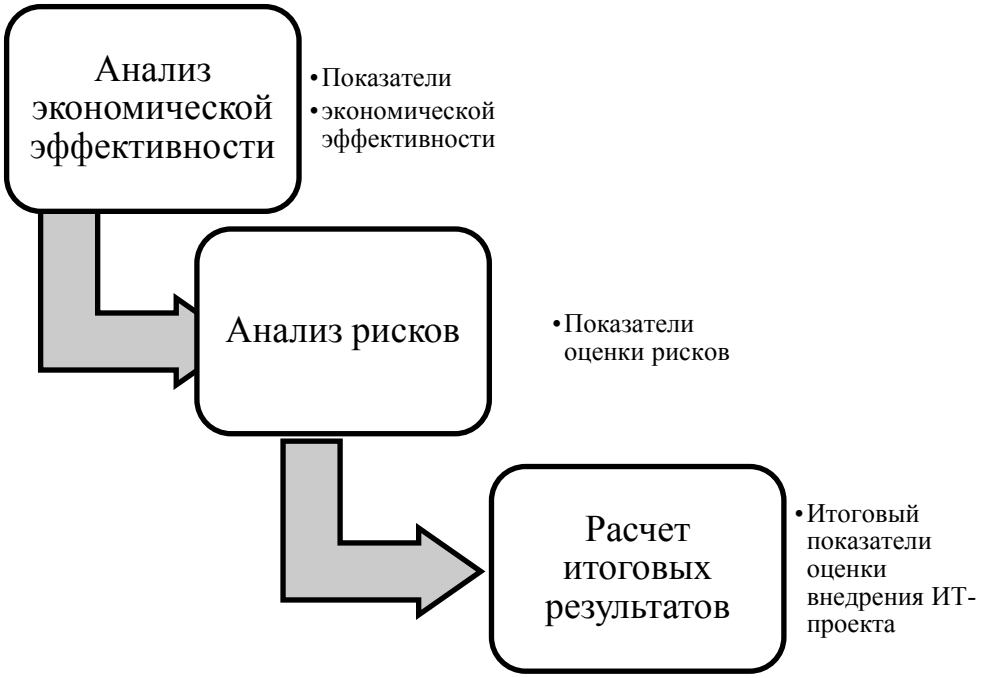


Рисунок 8 – Каскадная модель последовательности выполнения работ

Действия менеджера можно разделить на два последовательных этапа: анализ экономической эффективности и анализ рисков. Но можно проследить, что после выполнения последнего этапа возможен возврат к начальному. (Рисунок 8) [11].

2.5.3 Документирование прецедентов

Выгрузка файлов

Имя прецедента: Анализ экономической эффективности.

Сводка: Менеджер вводит необходимые данные об организации, существующей ИТ-инфраструктуре на предприятии и о планируемой ИТ-инфраструктуре. После этого анализирует полученные выгоды, затраты, а так же необходимые экономические показатели.

Зависимости: На основании данного прецедента проводится прецедент «Анализ рисков».

Актеры: Менеджер.

Предусловия: Получение доступа к данным провайдера и организации.

Описание (Таблица 2);

Таблица 2 – Описание прецедента «Анализ экономической эффективности»

Актер	Действие актера	Реакция системы
Менеджер	Получил доступ к данным	Автоматическое определение типов данных
	Указал нужные данные	Автоматический расчет результатов показателей экономической эффективности

Альтернативы: Невозможность расчёта экономической эффективности при отсутствии данных.

Пост-условие: Наличие данных от экспертов провайдеров и специалистов организации для оценки эффективности.

Неясные вопросы: возможность не согласования типа данных для модели.

Загрузка данных

Имя прецедента: Анализ рисков.

Сводка: Менеджер вводит необходимые данные о существующих рисках ИТ-системы. После этого анализирует полученные показатели оценки рисков и эффективности.

Зависимости: выполняется после прецедента «Анализ экономической эффективности».

Актеры: Менеджер.

Предусловия: Получение доступа к данным провайдера и организации.

Описание (Таблица 3);

Таблица 3 – Описание прецедента «Анализ рисков»

Актер	Действие актера	Реакция системы
Менеджер	Получил доступ к данным	Автоматическое определение типов данных
	Указал нужные данные	Автоматический расчет результатов показателей рисков, а так же итоговой эффективности от внедрения проекта

Альтернативы: Невозможность оценки итоговых результатов без оценки экономической эффективности.

Пост-условие: Наличие данных для оценки рисков.

Неясные вопросы: При проверке форматов данных произошло несовпадение [9].

3 Проектирование консолидированной модели

3.1 Функциональное обеспечение

3.1.1 Функциональная модель «как должно быть»

Использование предлагаемой модели должно позволить организациям максимально упростить процесс оценки эффективности ИТ-проекта. На рисунках 9, 10 показана функциональная модель процесса оценки эффективности ИТ-проекта «как должно быть», спроектированная с учетом данных требований [24].

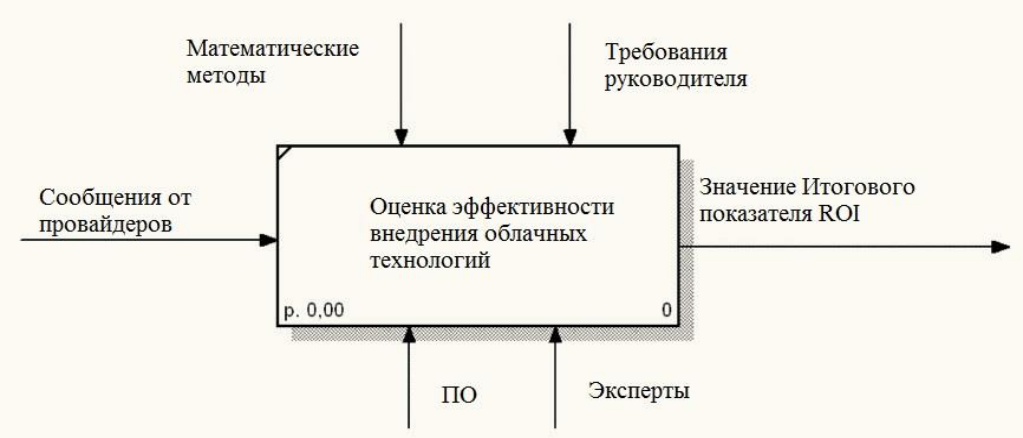


Рисунок 9 – Контекстная диаграмма функциональной модели «TO BE»

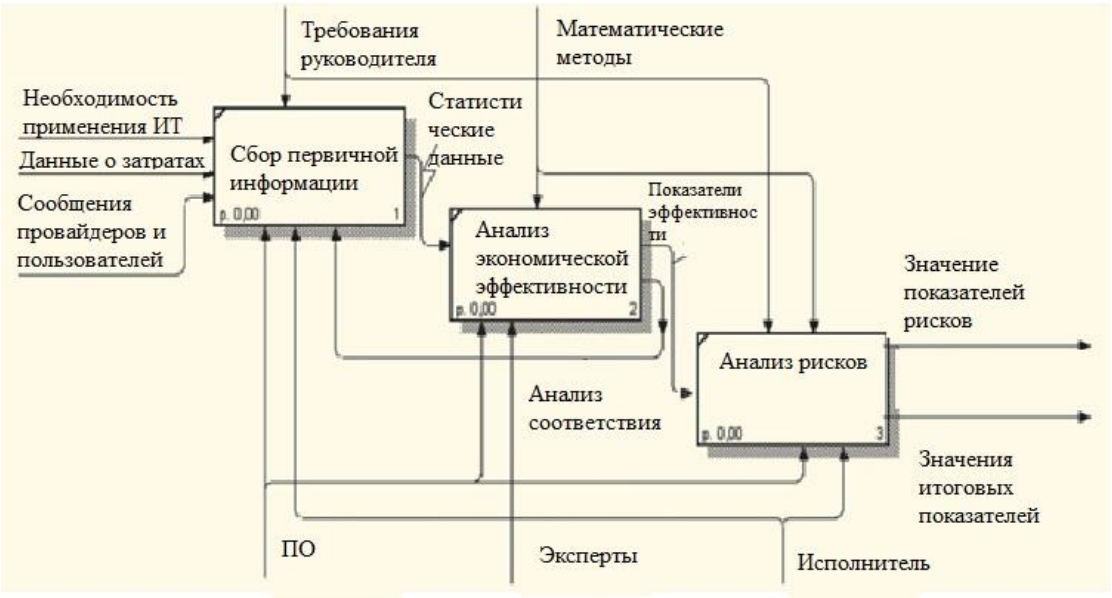


Рисунок 10 – Декомпозиция блока «Оценка эффективности ИТ-проекта»

Схема работы модели будет выглядеть следующим образом:

- сотрудниками организации производится сбор первичной информации о интересуемых рисках у провайдеров облачных услуг, а так информация, необходимая для расчета экономической эффективности;
- данная информация записывается в модель, где происходит экономическая оценка эффективности использования облачных технологий;
- далее рассчитывается вероятностная оценка каждого риска;
- на основании полученной информации рассчитываются основные критерии для оценивания рисков;
- на выходе получаем значения показателей, для оценки итоговых результатов по оценке эффективности и рисков использования облачных технологий [15].

3.1.2 Функциональная архитектура

Целью проектной части является проектирование процесса оценки рисков внедрения облачных технологий для консолидированной модели оценки эффективности, что позволит сократить временные затраты специалистов на оценивание эффективности внедрения ИТ-проекта и повысить качество оценки эффективности, учитывая особенности облачных технологий.

Рисунок 11 – Функциональная архитектура

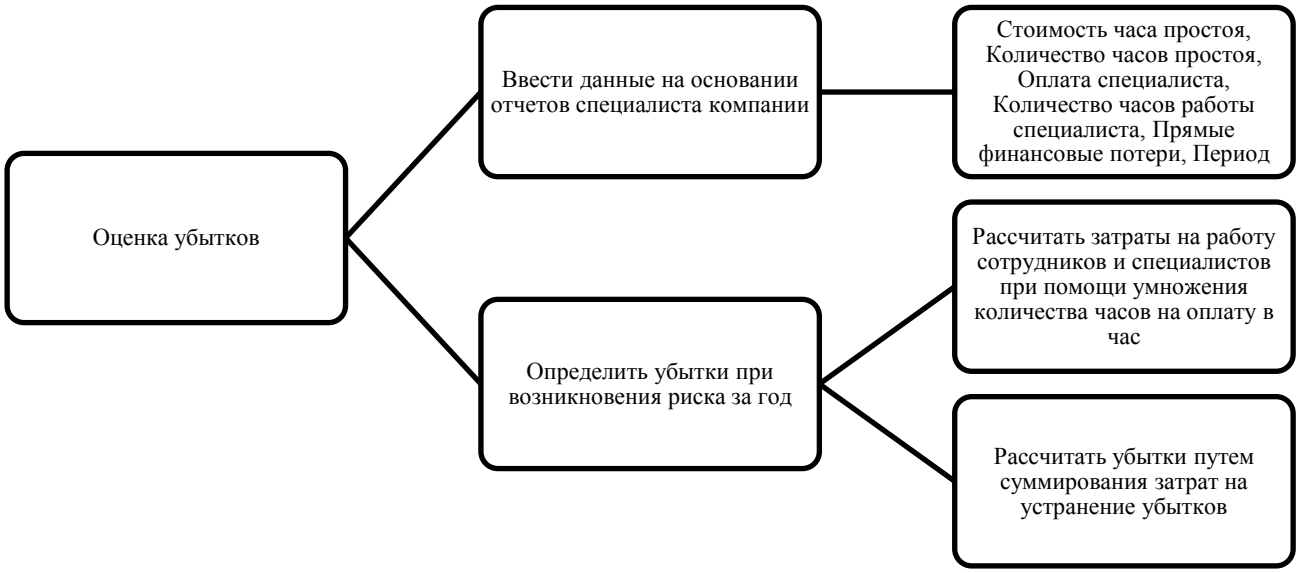


Рисунок 12 – Функциональная архитектура

Рисунок 13 – Функциональная архитектура

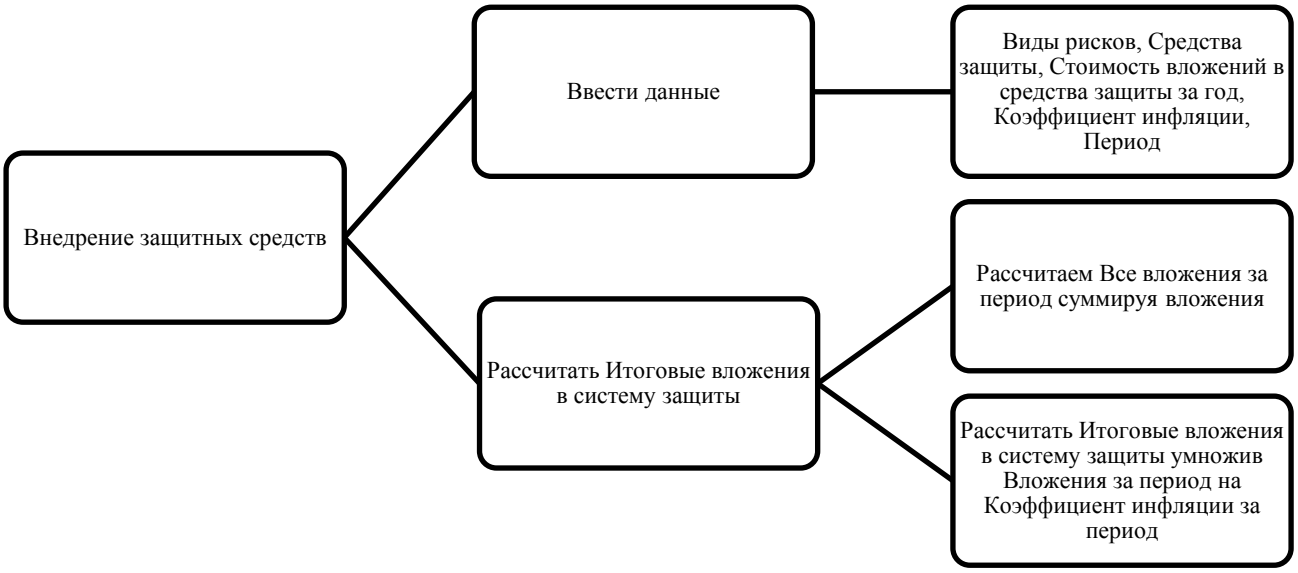


Рисунок 14 – Функциональная архитектура

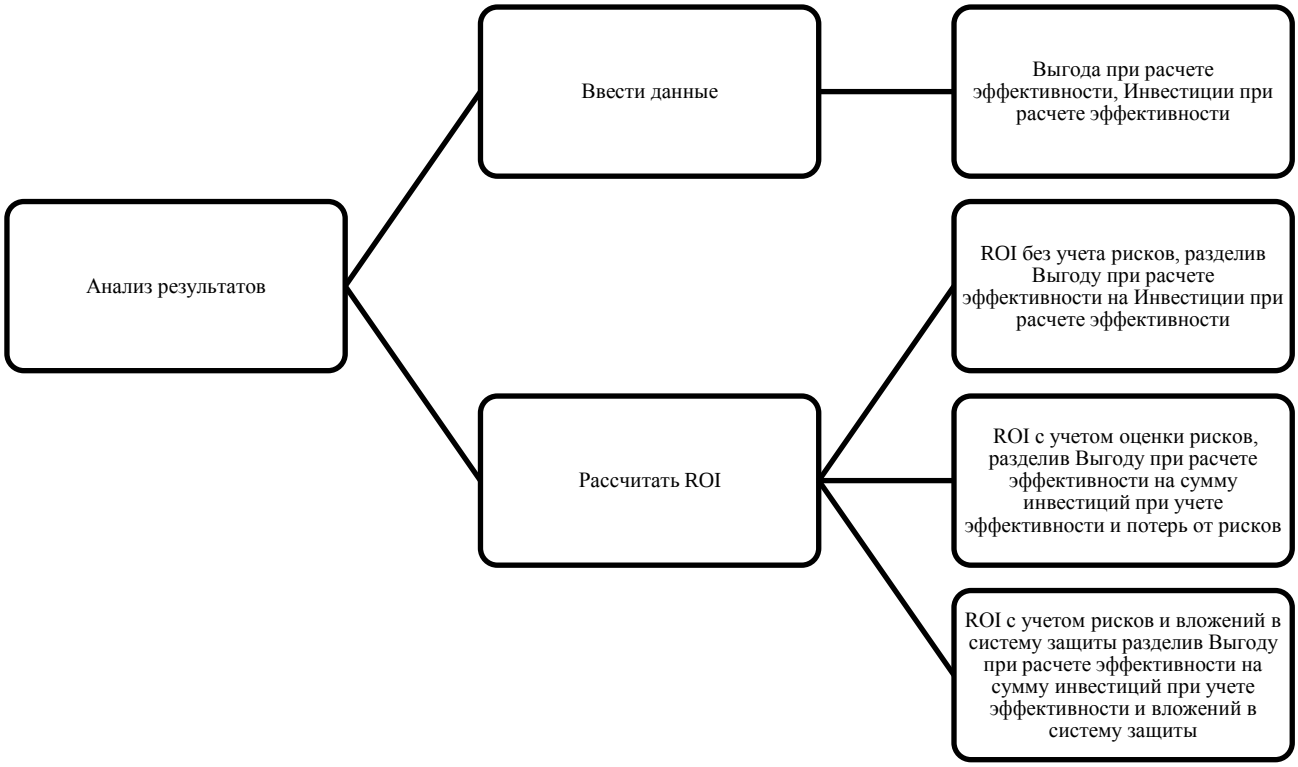


Рисунок 15 – Функциональная архитектура

Функциональная архитектура (совокупность функциональных подсистем, комплексов задач и процедур) – архитектура автоматизируемых бизнес-процессов – определяет состав функциональных подсистем и комплексов задач (в виде набора операций, функций, задач обработки информации), обеспечивающих реализацию бизнес-процессов.

Определим функциональную архитектуру проектируемого процесса оценки рисков на рисунках 11 - 15. [19]

3.2 Технологическое обеспечение

Технологическое обеспечение предполагает описание организации технологии сбора, передачи, обработки и выдачи информации.

Здесь описывается последовательность операций, начиная от способа сбора (получения) первичной информации (включающая данные, которые используются для корректировки нормативно-справочной информации, и оперативная информацию, используемая для расчетов), и заканчивая формированием результатной информации и способами ее передачи.

Спроектируем последовательность операций, которые будут осуществляться при оценивании рисков облачных технологий.

3.2.1 Диаграмма контекста системы

На «Диаграмме контекста» изображено взаимодействие пользователя Менеджера с системой «Оценка рисков» через «Интерфейс пользователя» (рисунок 16).

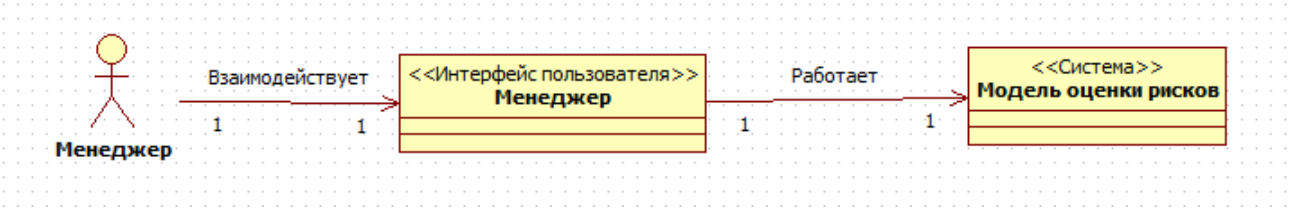


Рисунок 16 – Диаграмма контекста

Хотя контекстная диаграмма данных является лишь особым вариантом DFD, она играет важную роль в процессе проектирования систем и поэтому должна быть упомянута особо.

3.2.2 Диаграмма сообщений

Связи при переходе от одного объекта к другому отображаются на «Диаграмме Сообщений». На «Диаграмме сообщений» отражаются объекты, участвующие во взаимодействии друг с другом, и порядок отправки сообщений

(до/после) для каждого прецедента. Диаграммы строятся для каждого прецедента.

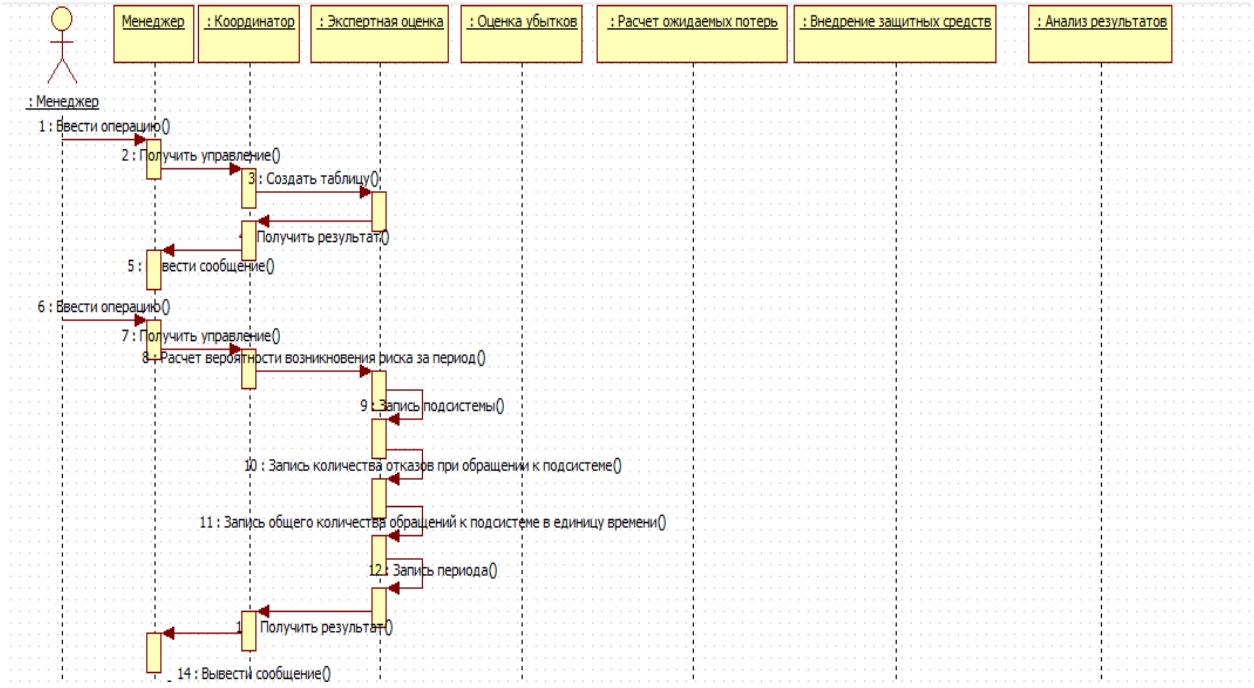


Рисунок 17 – Диаграмма сообщений для Прецедента «Экспертная оценка»

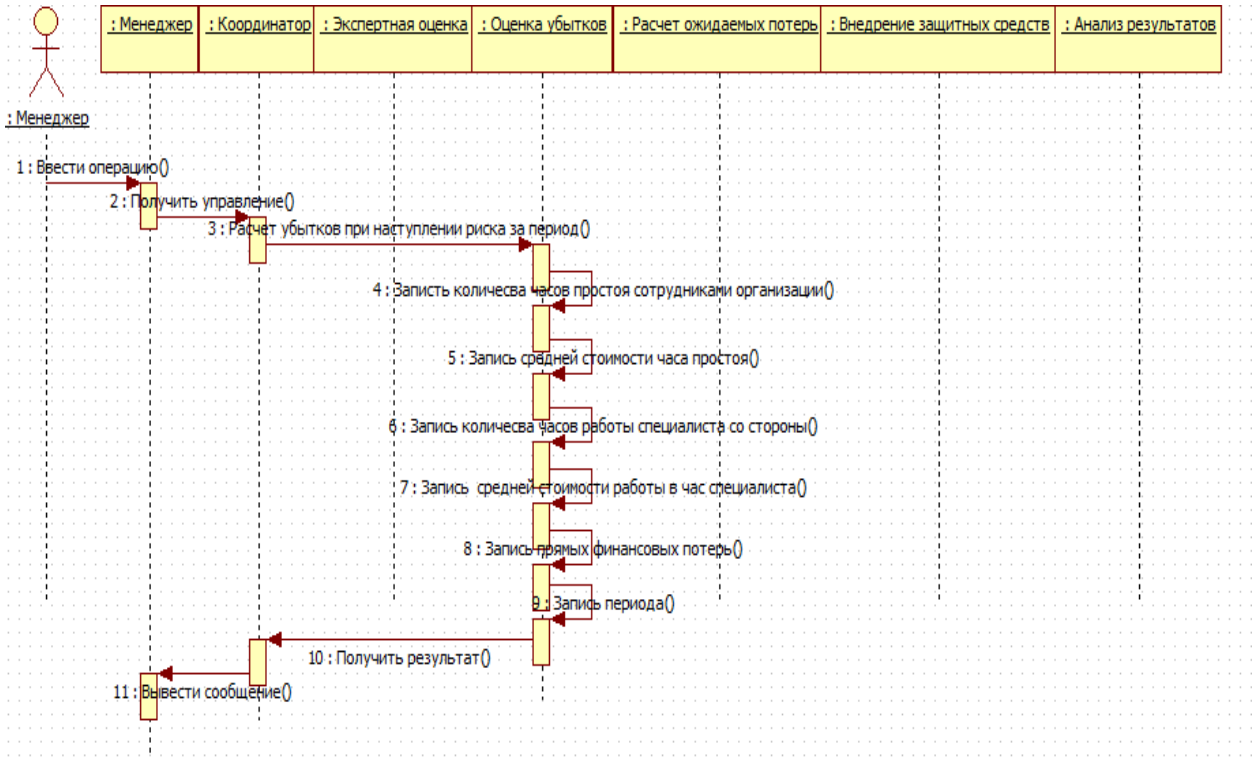


Рисунок 18 – Диаграмма сообщений для Прецедента «Оценка убытков»

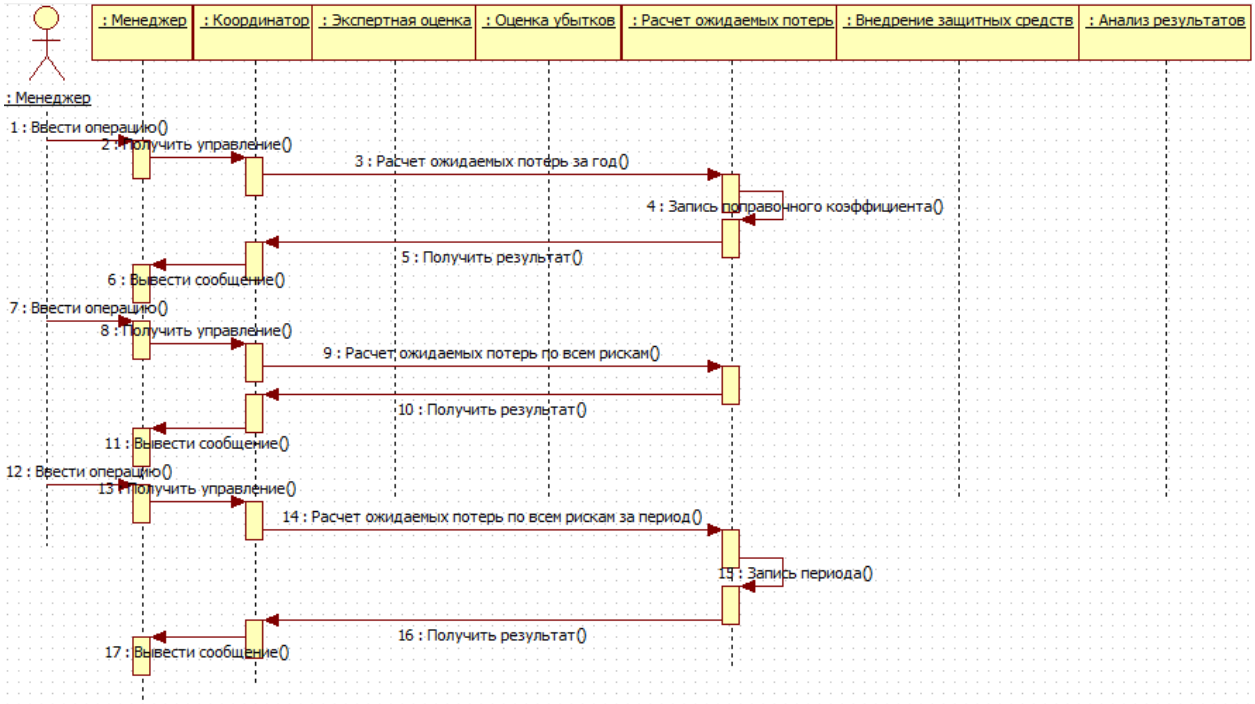


Рисунок 19 – Диаграмма сообщений для Прецедента «Ожидаемые потери при возникновении рисков»

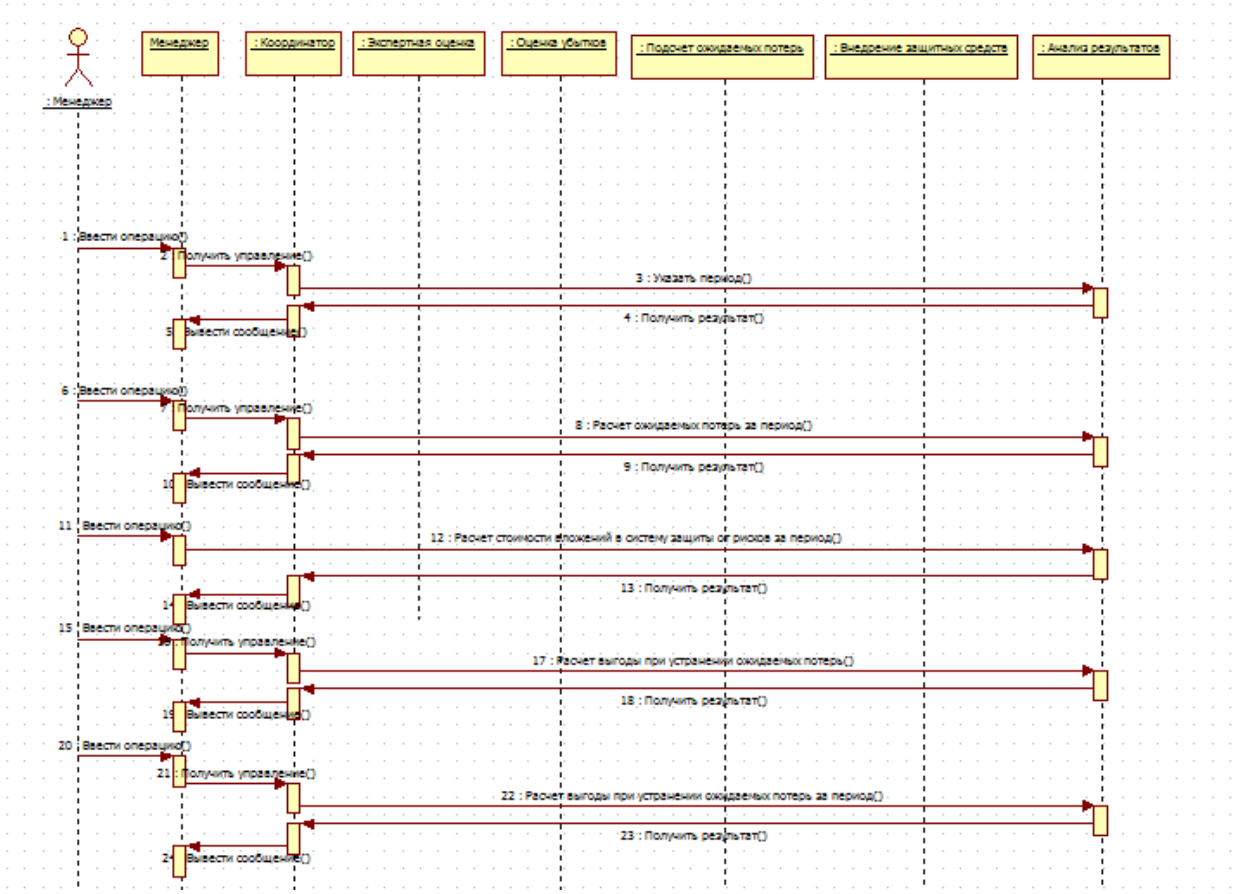


Рисунок 20 – Диаграмма сообщений для Прецедента «Внедрение средств защиты»

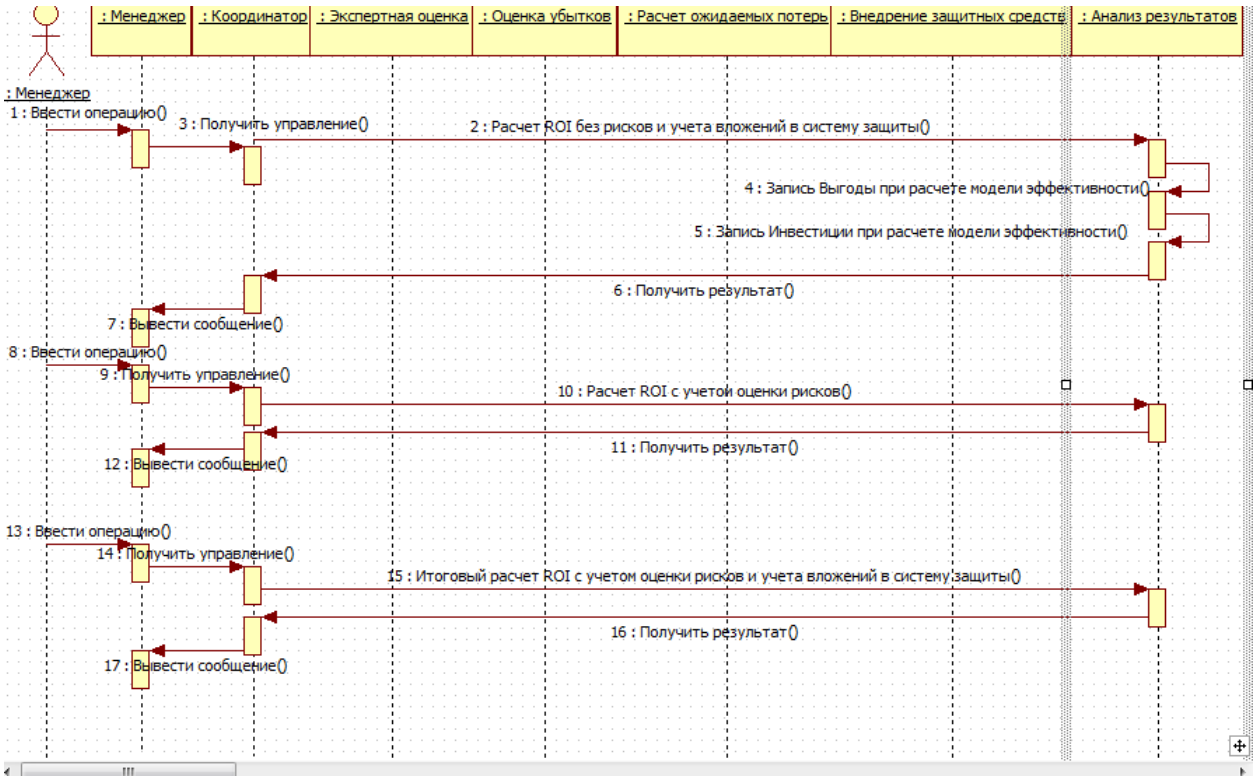


Рисунок 21 – Диаграмма сообщений для Прецедента «Анализ рисков»

Составим диаграммы последовательности, показывающие логическую цепочку событий, происходящих поочередно (рисунки 17 - 21). [25]

3.3 Информационное обеспечение

3.3.1 Построение диаграммы сущностных классов

Диаграмма сущностных классов служит для представления статической структуры модели системы. Диаграмма классов может отражать, в частности, различные взаимосвязи между отдельными сущностями предметной области, такими как объекты и подсистемы, а также описывает их внутреннюю структуру и типы отношений. (Рисунок 22). Опишем спецификацию интерфейса каждого класса, задействованного в разработке проекта. [7]

3.3.1 Обоснование выбора метода экспертной оценки

Получение знаний от экспертов является одной из главных трудностей при создании экспертных систем.

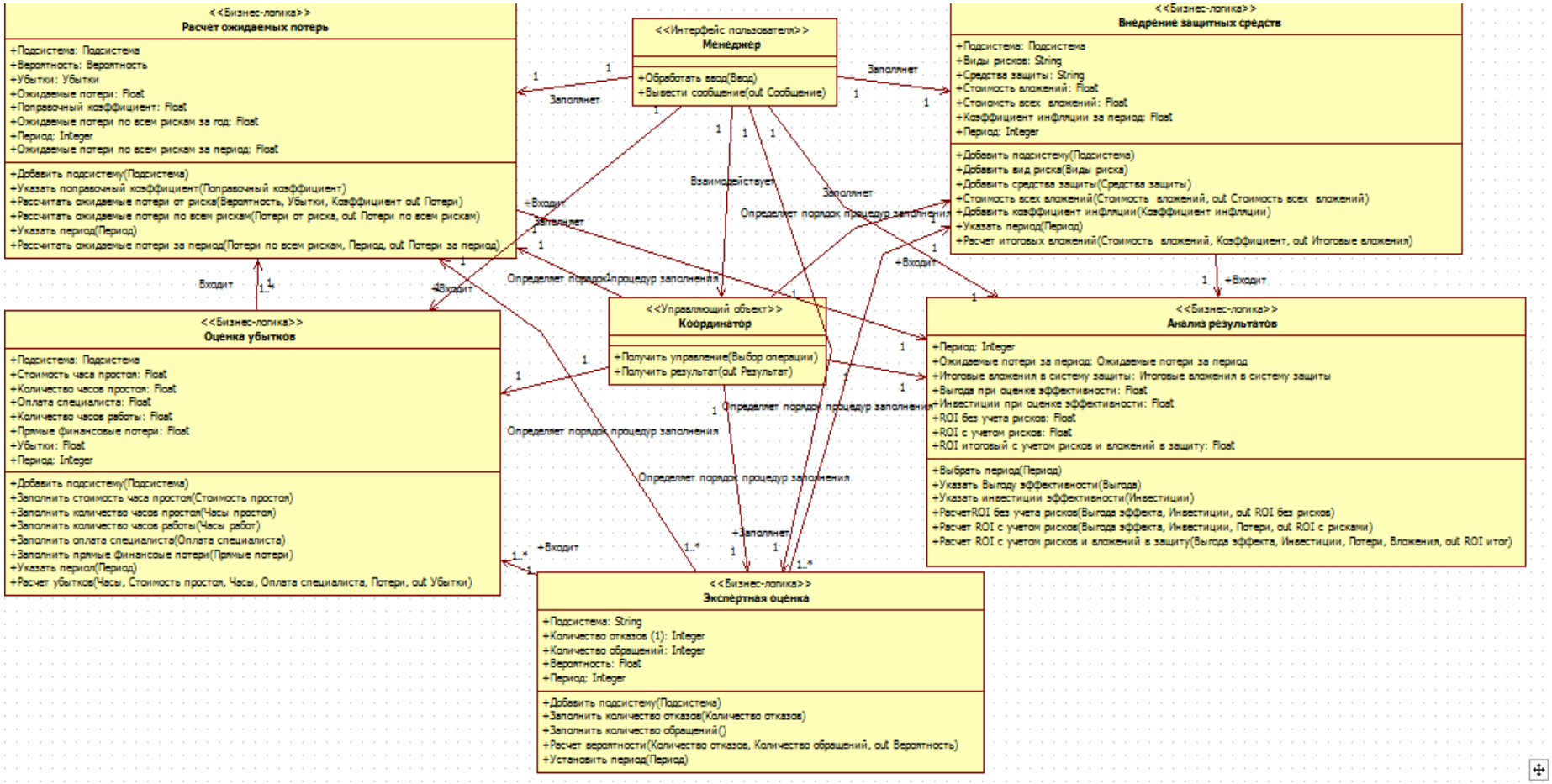


Рисунок 22 – Диаграмма сущностных классов

Существует несколько причин этого:

1. Использование экспертами узкоспециализированных терминов с неочевидным для неспециалиста смыслом.

2. Невозможность формализации в терминах математической теории большого числа знаний и фактов, используемых экспертом при решении задач.

3. Обширный контекст экспертного анализа: очень многие знания, используемые экспертом, кажутся ему само собой разумеющимися, но для постороннего отнюдь таковыми не являются.

4. Эксперты не хотят вводить данные в экспертную систему, мотивируя это недружественностью интерфейса.

5. Ни один эксперт не обладает полными знаниями в своей предметной области.

Выбор оптимального способа работы с экспертами поможет минимизировать эти недостатки.

В силу невозможности организовать групповую работу с экспертами, выбор будет производиться только между индивидуальны методами.

В процедуре извлечения знаний участвуют аналитик – специалист в области инженерии знаний и эксперт, у которого требуется извлечь знания.

Работа аналитика с экспертами проходит в 3 этапа.

1. Подготовительный этап. Для успеха общения оба участника должны тщательно подготовиться к диалогу или игре. Желательно, чтобы эксперт был не только компетентным специалистом, но и заинтересованным (морально или материально) лицом в достижении конечной целипостроении информационной системы. Он должен быть доброжелателен к аналитику и уметь объяснять свои знания (желательно, чтобы эксперт имел опыт преподавательской работы).

2. Установление «общего кода». Для создания лингвистического альянса взаимодействия участники взаимодействия должны пытаться сократить расстояние между объектом (т. е. исследуемой предметной областью) и аналитиком. Необходимо определить главные понятия, т. е. выработать

словарную основу базы знаний; уровень детализации; взаимосвязи между понятиями.

3. Гносеологический этап. На этом этапе происходит выяснение закономерностей, присущих предметной области, условий достоверности и истинности утверждений, структурирование за счет введения отношений. Этот этап является определяющим во взаимодействии аналитика и эксперта. В процессе анализа игры или диалога вербализуется и формализуется знание эксперта и зачастую для него самого порождается новое знание.

Индивидуальные методы извлечения знаний подразделяются на пассивные и активные.

Пассивные методы заключаются в том, что главная роль в извлечении знаний отдается эксперту, а аналитик отвечает за процесс сохранения и систематизации полученных результатов. В группу пассивных методов включаются наблюдения и лекции.

В методе наблюдений аналитик выступает в роли наблюдателя, а эксперт выполняет свою повседневную работу, поясняя вслух все, что он делает. Наблюдение исключает любую возможность обратной связи аналитика с экспертом, чтобы не повлиять на процесс и не исказить получаемые результаты. Наблюдение эксперта на его рабочем месте не всегда может быть, возможно, так как его работа может требовать конфиденциальности, что не позволяет присутствие посторонних во время процесса. В таком случае, наблюдение производится во время имитации рабочего процесса.

Метод практически не автоматизируемый, всю обработку результатов аналитик вынужден выполнять самостоятельно, без поддержки технических средств. Все полученные данные могут быть приняты или не приняты во внимание только по усмотрению аналитика. Полученное знание сильно фрагментировано. Аналитику необходимо создать систему смыслов из разрозненной информации, отражающей единичный опыт, поэтому полученное знание, как правило, будет не полным.

При применении метода лекций эксперту ставят задачу составить, хорошо структурировать, и провести лекцию. Задача аналитика прослушать лекцию и составить структурированную информацию об исследуемой области.

Из пассивных методов лекции более предпочтительны, но хороших лекторов, которые способны доходчиво подать материал, очень мало. Так же на лекциях аналитик вынужден больше слушать, а не задавать вопросы, что уменьшает силу обратной связи с экспертом.

Пассивные методы не могут быть полностью автоматизированы. Информация получаемая этими методами разнородная и не полная, что требует высоких интеллектуальных затрат эксперта по ее систематизации и формирования знания.

В активных методах извлечения знаний аналитик составляет сценарии сеансов извлечения знаний и в большей степени управляет всем процессом, нежели эксперт. Эти методы наиболее распространены в сфере инженерии знаний.

В группу индивидуальных активных методов включаются анкетирование, интервью и свободный диалог.

В случае анкетирования аналитик составляет анкету и просит заполнить ее одного или несколько экспертов. Анкета не должна быть скучной и однообразной, а язык изложения вопросов в ней должен быть понятен экспертам. Заполнение анкеты предпочтительнее поручить экспертам, так как это даст больше времени на обработку результатов.

Основной недостаток анкет состоит в том, что вопросы могут быть не правильно поняты экспертом.

Метод интервью представляет собой специфическую форму общения. Имеет сходство с анкетированием, в котором аналитик сам заполняет анкету, но в процессе может некоторые вопросы опустить и добавить новые.

Метод интервьюирования отличается от метода анкетирования тем, что позволяет аналитику опускать ряд вопросов в зависимости от ситуации,

вставлять новые вопросы в анкету, изменять темы и разнообразить ситуацию общения.

Свободный диалог. Метод заключается в беседе эксперта и аналитика. Процесс требует тщательно подготовки аналитика. Он должен составить план, который должен учитывать заинтересовывающее начало, извлечение знаний на последующем и этапе и в заключении благодарность эксперту за потраченное его время. Сравнение активных индивидуальных методов представлено в таблице 4.

В случае разрабатываемой системы оптимальным методом извлечения знаний является интервью.

В основу интервью целесообразно положить один из методов экспертного оценивая, в данном случае индивидуальный экспертный опрос.

Таблица 4 – Сравнение активных индивидуальных методов

Показатели	Анкетирование	Интервьюирование	Свободный диалог
Достоинства	Возможность стандартизированного опроса нескольких экспертов. Не требует особенного напряжения от аналитика во время процедуры анкетирования	Наличие обратной связи (возможность уточнения контекста и разрешения противоречий)	Гибкость Обратная связь Возможность изменения сценария и формы сеанса
Характеристика предметной области	Слабоструктурированные, слабодокументированные и среднедокументированные предметные области.		

Индивидуальный экспертный опрос – это опрос в форме интервью или в виде анализа экспертных оценок. Означает беседу заказчика с экспертом, в ходе которой заказчик ставит перед экспертом вопросы, ответы на которые значимы для достижения программных целей. Анализ экспертных оценок предполагает индивидуальное заполнение экспертом разработанного заказчиком формуляра, по результатам которого производится всесторонний анализ проблемной ситуации и выявляются возможные пути ее решения. Свои соображения эксперт выносит в виде отдельного документа.

3.3.3 Характеристика критериев оценки рисков

CloudSecurityAlliance (CSA), некоммерческая отраслевая организация, продвигающая методы защиты в облаке, предоставила отчет о главных угрозах, возникающих при пользовании облачными услугами.

CSA указывает, что отчет отражает согласованное мнение экспертов о наиболее значительных угрозах безопасности в облаке и уделяет основное внимание угрозам, проистекающим из совместного использования общих облачных ресурсов и обращения к ним множества пользователей по требованию.

Целью публикации данного отчета является предоставление помощи пользователям облака и поставщикам облачных услуг при внедрении лучших стратегий снижения риска.

На основании данного отчета выделим основные подсистемы, в которых могут возникнуть угрозы, так же охарактеризуем риски и выявим способы их предотвращения (рисунок 23).

Риск «Кража данных»

Кража конфиденциальной корпоративной информации - всегда страшит организации при любой ИТ-инфраструктуре, но облачная модель открывает «новые, значительные магистрали атак», указывает CSA. «Если база данных облака с множественной арендой не продумана должным образом, то изъян в приложении одного клиента может открыть взломщикам доступ к данным не только этого клиента, но и всех остальных пользователей облака», - предупреждает CSA.

У любого «облака» есть несколько уровней защиты, каждый из которых защищает информацию от разного типа «покушений».

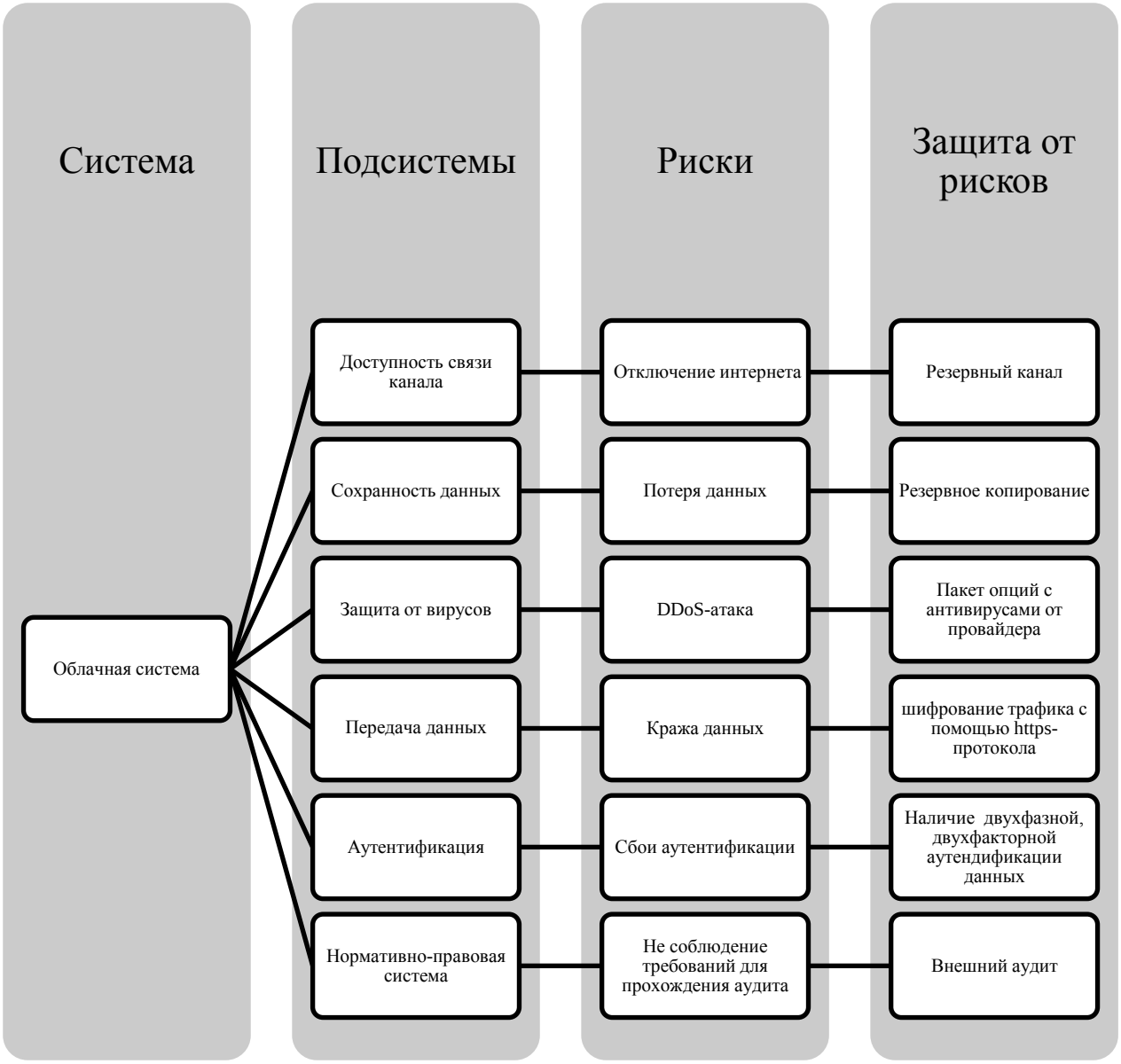


Рисунок 23 – Система оценки рисков

Так, например, физическая защита сервера. Здесь речь идет даже не о взломе, а о воровстве или порче носителей информации. Вынести сервер из помещения может быть тяжело в прямом смысле этого слова. Кроме этого, любая уважающая себя компания хранит информацию в дата-центрах с охраной, видеонаблюдением и ограничением доступа не только посторонним, но и большинству сотрудников компании. Так что вероятность того, что злоумышленник просто придет и заберет информацию, близка нулю.

Подобно тому, как опытный путешественник, опасаясь ограблений, не хранит все деньги и ценности в одном месте, SaaS-компании не держат всю информацию на одном сервере. Так, взлом, даже если он произойдет,

становится куда менее болезненным. Чем он грозит пользователю? Практически, ничем. Как показывает практика, чаще всего ври взломе сервера воруют базу email-адресов. Это значит, что пользователь получит на почтовый ящик долю спама. И всё.

Второй уровень защиты «облаков» – это защита в процессе передачи данных. SaaS-компании шифруют весь траффик с помощью https-протокола с использованием SSL-сертификата. Так данные будут в безопасности от попыток анализаторов траффика перехватить их.

Риск «Потеря данных»

Данные, хранящиеся в облаке, могут быть украдены злоумышленниками или потеряны по другой причине, пишет CSA. Если поставщик облачных услуг не внедрит должные меры резервного копирования, данные случайно может удалить сам провайдер или они пострадают при пожаре или стихийном бедствии. С другой стороны, заказчик, который шифрует данные до того, как выгрузить их в облако, вдруг потерявший шифровальный ключ, также утратит свои данные, добавляет CSA.

Опасение обосновано, но проблем можно избежать резервным копированием. Компании, которые заботятся о клиентах и о репутации, ежедневно и не менее двух раз автоматически копируют базу данных. Таким образом, если пользователь обратиться в техподдержку с сообщением о случайно удаленных, но важных файлах, их можно будет восстановить.

Такая проблема также должна решаться превентивно, со стороны пользователя, и относится к вопросу инструктажа и компьютерной грамотности коллег, а также ограничением прав доступа к изменению и удалению файлов.

Риск «DDoS-атаки»

На облако могут быть предприняты атаки типа «отказ в обслуживании», которые вызывают перегрузку инфраструктуры, заставляя задействовать огромный объем системных ресурсов и не давая заказчикам пользоваться этой услугой. Внимание прессы чаще всего привлекают распределенные, или DDoS-атаки, но есть и другие типы DoS-атак, которые могут блокировать облачные

вычисления, пишет CSA. К примеру, злоумышленники могут запустить асимметричные DoS-атаки прикладного уровня, используя уязвимости в Web-серверах, базах данных или других облачных ресурсах, чтобы завалить приложение с очень малой полезной нагрузкой.

Избежать данного риска можно при подключении специального Пакета опций с антивирусами, который должен предоставить любой, уважающий себя провайдер.

Риски в «Нормативно-правовой системе»

Под данным риском предполагается степень использования провайдером законов и правил, применимых к сфере облачных вычислений, а именно соблюдение следующих регулятивных норм:

подтверждение соответствия существующим нормам, где бы ни находились данные;

разработка комплексной политики по управлению данными и по соблюдению законодательных требований;

реализация средств надлежащего контроля;

высокий уровень соответствия требованиям, обеспечиваемый поставщиком облака;

предоставление необходимой документации от провайдера заказчику о соблюдении требований для прохождения аудита;

предоставление документации о соблюдении требований в отношении рабочих нагрузок, запущенных в облаке.

Риск нарушения «Аутентификации»

Для того, чтобы избежать кражи аккаунтов, взлома услуг, и т. д. обязательно нужно включить двухэтапную аутентификацию. Это означает, что после ввода пароля пользователю на телефон будет отправлен специальный код подтверждения, который необходимо будет ввести в специальное поле после авторизации. Без него, даже с правильным паролем, получить доступ к аккаунту не удастся. Таким образом, система предупредит вас в случае, когда кто-то захочет получить несанкционированный доступ к вашей учетной записи.

Двухфакторная система безопасности основана на том, что пользователь, кроме того, что знает пароль доступа к определенному имени пользователя («логину»), – владеет и инструментом для получения соответствующего ему ключа доступа. Последним может служить сохраненный на компьютере электронный сертификат безопасности либо пришедший на личный телефон СМС с кодом подтверждения, либо же отпечаток пальца, снятый считывающим электронным устройством [23].

3.4 Аппаратное обеспечение

Модель оценки рисков может использоваться на компьютере с операционной системой MicrosoftWindows, а так же офисным пакетом MicrosoftOffice в табличном редакторе MicrosoftExcel.

3.5 Руководство пользователя

Опишем основные функции при использовании Консолидированной модели оценки эффективности использования облачных технологий.

	A	B	C	D	E
1	**Экспертная оценка**				
2	**Подсистема**	**Количество отказов**	**Общее количество обращений к подсистеме в единицу времени**	**Вероятность возникновения риска (от 0 до 1)**	**Период (Количество лет)**
3	Доступность канала связи	10	4350	0,002	1
4	Сохранность данных	4	3740	0,001	
5	Защита от вирусов	5	4350	0,001	
6	Передача данных	8	6821	0,001	
7	Аутентификация	11	2364	0,005	
8	Нормативно-правовая подсистема	3	1453	0,002	
9					

Рисунок 24 – Интерфейс для Прецедента «Экспертная оценка»

Экспертная оценка (рисунок 24):

выберем подсистемы, в которых необходимо оценить риски;

проведем сбор первичной информации по каждой подсистеме у экспертов;

заполним колонки Количество отказов и Общее количество обращений к системе в единицу времени;

укажем, за какой период (в годах) рассматривается система;

оценим полученный результат в колонке Вероятность возникновения риска.

	A	B	C	D	E	F	G	H
1	**Оценка убытков при возникновении риска**							
2	**Подсистема**	**Стоимость часа простоя (рубли)**	**Количество часов простоя**	**Оплата специалиста (рубли)**	**Количество часов работы специалиста**	**Прямые финансовые потери (рубли)**	**Убытки за год (рубли)**	**Период (Количество лет)**
3	Доступность канала связи	10000	8				80000	1
4	Сохранность данных	200	160				110000	
5	Защита от вирусов			500	3	80000	81500	
6	Передача данных					40000	40000	
7	Аутентификация					50000	50000	
8	Нормативно-правовая подсистема			2000	4	15000	23000	
9								

Рисунок 25 – Интерфейс для Прецедента «Ожидаемые потери при возникновении рисков»

1. Оценка убытков (рисунок 25):

- проведем сбор первичной информации по каждой подсистеме у специалистов организации;
- заполним следующие колонки (в рублях): Стоимость часа простоя, Количество часов простоя, Оплата специалиста, количество часов работы специалиста, Прямые финансовые потери
- укажем, за какой период (в годах) рассматривается система;
- оценим полученный результат в колонке Убытки.

2. Ожидаемые потери при возникновении риска (рисунок 26):

Ожидаемые потери при возникновении риска

Подсистема	Вероятность возникновения риска от 0 до 1	Убытки (рубли)	Поправочный коэффициент от 0 до 1	Ожидаемые потери за год (рубли)	Ожидаемые потери по всем рискам за год (рубли)	Период (количество лет)	Ожидаемые потери по всем рискам за период (рубли)
Доступность канала связи	0,002298851	80000	1	183,908046	722,2916783	5	3611,458391
Сохранность данных	0,001069519	110000	1	117,6470588			
Защита от вирусов	0,001149425	81500	1	93,67816092			
Передача данных	0,001172849	40000	1	46,91394224			
Аутентификация	0,00465313	50000	1	232,6565144			
Нормативно-правовая подсистема	0,002064694	23000	1	47,48795595			

Рисунок 26 – Интерфейс для Прецедента «Ожидаемые потери при возникновении рисков»

- укажем поправочный коэффициент, который позволяет учесть, что в результате реализации угрозы защищаемый ресурс может быть уничтожен не полностью, а только частично;
- оценим Ожидаемые потери за год;
- ожидаемые потери по всем рискам за год;
- укажем, за какой период (в годах) рассматривается система;
- оценим Ожидаемые потери по всем рискам за период.

3. Внедрение защитных средств (рисунок 27):

Внедрение защитных средств

Подсистема	Виды рисков	Пример средств защиты	Вложения в средства защиты за год (рубли)	Все вложения за период (рубли)	Коэффициент инфляции за период в %	Период, за который рассчитываются затраты на внедрение (количество лет)	Итоговые вложения в систему защиты
Доступность канала связи	Отключение интернета	Резервный канал	10000	80000	7	5	85600
Сохранность данных	Потеря данных						
Защита от вирусов	Вирусная атака	Пакет опций с антивирусами от провайдера	7000				
Передача данных	Потеря данных		20000				
Аутентификация	Сбои аутентификации	Наличие двухфазной аутендификации данных	40000				
Нормативно-правовая подсистема	Нормативно-правовая подсистема	Внешний аудит	3000				

Рисунок 27 – Интерфейс для Прецедента «Внедрение средств защиты»

- при помощи экспертов, специалистов компании, руководства организации определяем какие риски нужно учесть в каждой подсистеме и каким способом предотвратить их;

- записываем результаты в колонки Виды рисков и Пример средств защиты;
- результаты расчетов специалистами о количестве денежных средств (в рублях), которые нужно вложить в защиту системы указываем в колонку Вложения в средства защиты за год;
- Указываем Коэффициент обесценивания денег, рассчитанный специалистами организации, в нашем случае для примера это Коэффициент инфляции;
- оцениваем Все вложения за период;
- укажем, за какой период (в годах) рассматривается система;
- оценим Итоговые вложения в систему защиты с учетом инфляции за выбранный период.

4. Анализ результатов за период (рисунок 28):

В результате инвестиций в решения EMC планируется достичь следующих результатов:		
Общая выгода	51 773 500	USD
Чистая выгода за Пять лет	21 617 111	USD
Объем инвестиций за Пять лет	30 156 388	USD
Возврат на инвестиции - ROI (чистая выгода / общий объем инвестиций)	72%	
Чистая приведенная выгода (NPV)	10 909 504	USD
Период окупаемости (месяцев)	23	мес.
IRR	38%	

Рисунок 28 – Интерфейс модели оценки эффективности внедрения

- рассчитаем Чистую выгоду и Объем инвестиций за пять лет при помощи модель оценки эффективности внедрения виртуальных и облачных сред на базе технологий EMC/VMware (рисунок 29);

	A	B	C	D	E
1	**Анализ результатов за период**				
2	**Период (количество лет)**	**Ожидаемые потери (рубли)**	**Итоговые вложения в систему защиты (рубли)**	**Выгода при расчете эффективности (рубли)**	**Инвестиции при расчете эффективности (рубли)**
3	5	3611,458391	85600	215000	320000
4					
5					
6	**Показатель ROI**	**Значение**			
7	ROI без учета рисков	0,671875			
8	ROI с учетом оценки рисков	0,664376969			
9	ROI с учетом рисков и вложений в систему защиты	0,530078895			
10					

Рисунок 29 – Интерфейс для Прецедента «Анализ рисков»

- заполним колонки (в рублях) в модели рисков Выгода при расчете эффективности и Инвестиции при расчете эффективности;
- оценим коэффициент ROI без учета рисков;
- оценим коэффициент ROI с учетом оценки рисков;
- оценим коэффициент ROI с учетом рисков и вложений в систему защиты.
- Если значение ROI больше единицы (ROI > 1), то это говорит о финансовой выгоде от совершенных инвестиций, если значение меньше единицы (ROI < 1), то это означает, что совершенные вложения не являются выгодными для организации, они убыточны. Если же ROI = 1, то затраты только окупаются.

3.6 Оценка эффективности ИТ-проекта

Принимая решение об инвестировании средств в ИТ-проект или иной другой, необходимо оценить его экономическую эффективность. Для этого разработаны средства автоматизации - программы инвестиционного анализа, моделирующие развитие проекта. При выборе таких программ необходимо четко представлять себе их возможности и особенности.

На российском рынке наиболее распространены несколько программ (таблица 5), в основе которых лежат классические подходы к оценке инвестиций. Разработчики этих пакетов регулярно выпускают новые, более гибкие версии, ежегодно увеличивая число пользователей. Существуют также менее известные программные пакеты, созданные на основе электронных таблиц и разработанные, как правило, консалтинговыми фирмами.

Во всех программных продуктах для анализа инвестиционных проектов методика и общие подходы к расчетам примерно одинаковы. Поэтому правильнее рассматривать такие пакеты как некие инструменты, каждый из которых применим в конкретной ситуации. Сегодня функциональные возможности последних версий пакетов для расчетов инвестиционных проектов находятся примерно на одном уровне [18].

Таблица 5 – Сравнительный анализ существующих пакетов программ для оценки инвестиционных проектов

Показатели/ Программы	Инструментальные средства разработки	Наличие специального инструментария для оценки облачных технологий
Модель оценки эффективности Облачных сред	Excel	Наличие
Project Expert	FoxPro	Отсутствует
Альт-Инвест	Excel	Отсутствует
ТЭО-Инвест	Excel	Отсутствует
Инвест-Проект	Excel	Отсутствует
FOCCAL-UNT	Excel	Отсутствует

На настоящий момент все программные продукты позволяют:

- разработать детальный финансовый план и оценить потребность в денежных средствах в будущем;
- определить схему финансирования инвестиционного проекта;
- оценить возможность и эффективность привлечения денежных средств из различных источников финансирования;
- разработать план производства и развития предприятия;
- определить эффективную стратегию маркетинга и рационального использования материальных, трудовых и финансовых ресурсов;
- рассчитать и проанализировать различные сценарии развития проекта, варьируя значения факторов, способных повлиять на финансовые результаты;
- контролировать процесс реализации инвестиционного проекта [13].

Проанализировав упомянутые программы в таблице 5, мною было принято решение о использовании готового инструмента моделирования, созданного специально для осуществления расчётов ROI при внедрении облачных технологий. Данный инструмент моделирования предназначен для оценки затрат и расчета экономической эффективности проектов консолидации систем управления контентом и оптимизации бизнес-процессов на базе технологий и решений EMC, VMware, Documentum. Инструмент реализован средствами MicrosoftExcel и предназначен для прогнозного моделирования

возврата инвестиции ROI в сценарии повышения эффективности управления контентом и бизнес-процессами коммерческих и государственных организаций.

Модель включает подробную оценку выгод для серверной и клиентской виртуализации, которая позволят руководителю отметить, насколько выгодными будут вложения в облачные технологии для его предприятия [14].

За основу данной модели принят Индекс рентабельности инвестиций, ROI, который указывает относительное превышение выгоды, которую мы получим, над первоначальными вложениями капитала. Показатель отдачи от инвестиций является одним из наиболее часто применяемых методов оценки эффективности инвестиций.

Формула расчета ROI облачных сервисов будет выглядеть следующим образом (1):

$$ROI = \frac{Доход - Инвестиции}{Инвестиции} * 100\% \quad , \qquad (1)$$

где: размер инвестиций – это все вложения предприятия на внедрение IT-проекта; а доход от инвестиций – получение прибыли от внедрения IT-проекта.

Другими словами, единственное, что нужно знать, для использования этой формулы – доход от инвестиций. Это не всегда так просто определить и перевести в деньги. Поэтому рассмотрим примеры основных показателей, которые необходимо учитывать при нахождении переменной доход от инвестиций при расчете эффективности облачных технологий с помощью метода ROI:

- оценка затрат на основные серверы;
- оценка затрат на питание и охлаждение основных серверов;
- оценка площади, занимаемой основными серверами;
- оценка затрат на развертывание основных серверов;
- оценка затрат на установку, настройку и обновление клиентских устройств;
- оценка трудозатрат на возобновление работы пользователей после аварий;

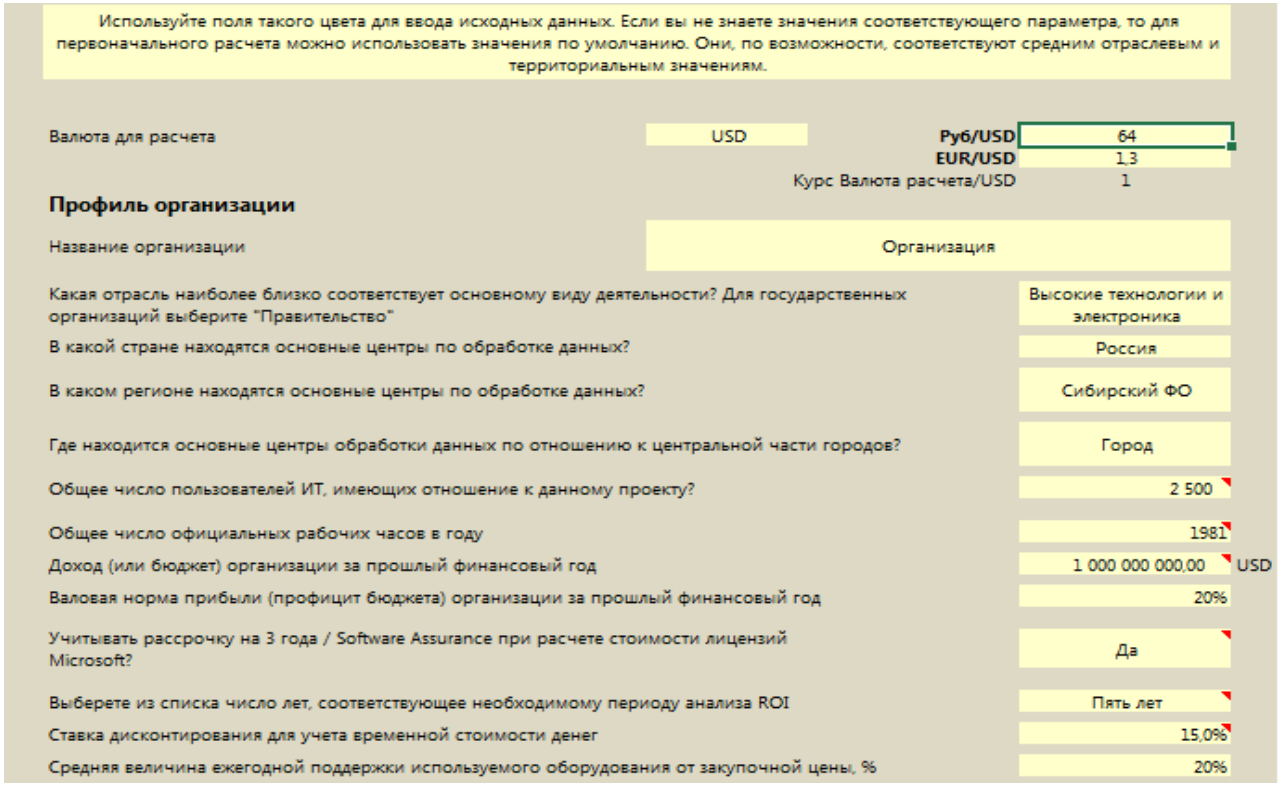
- оценка IT-затрат на управление изменениями по запросам пользователей в облачной инфраструктуре;
- оценка продуктивности пользователей облачной системы и т. д.

Для каждого из параметров будут определяться следующие критерии эффективности [17]:

- текущие значения («как есть») до внедрения облачных технологий;
- плановые значения («как будет») после внедрения проекта;
- реализация выгоды от проекта в процентах;
- реализация выгоды от проекта с учетом выполнения проекта в денежных единицах;
- чистая экономия («как есть» минус «как будет»);
- в случае отказа от использования, какой доли уже понесенных затрат можно избежать при помощи предлагаемого решения в процентах.

Но оценивая эффективность с помощью ROI, мы можем рассматривать полученные данные только как первый этап по оценке затрат и выгод от внедрения ИТ. Ведь помимо выгоды от проектов руководству важны риски, которые подразумевают нововведения в организацию. Так же в первоначальной модели не используются методы оценки внедрения защитной системы для предотвращения возникновения рисков, хотя их оценка весьма целесообразна. Этим предопределена необходимость проведения дальнейших исследований по развитию и детализации методов по оценке экономической эффективности от внедрения ИТ-проектов, в частности оценки эффективности применения облачных ИТ-сервисов в корпоративных информационных системах с учетом факторов риска.

Для получения наиболее объективной оценки результатов внедрения облачных технологий расширим существующую модель оценки эффективности внедрения виртуальных и облачных сред на базе технологий EMC/VMware, добавив показатели оценки рисков применения облачных ИТ-сервисов [4].



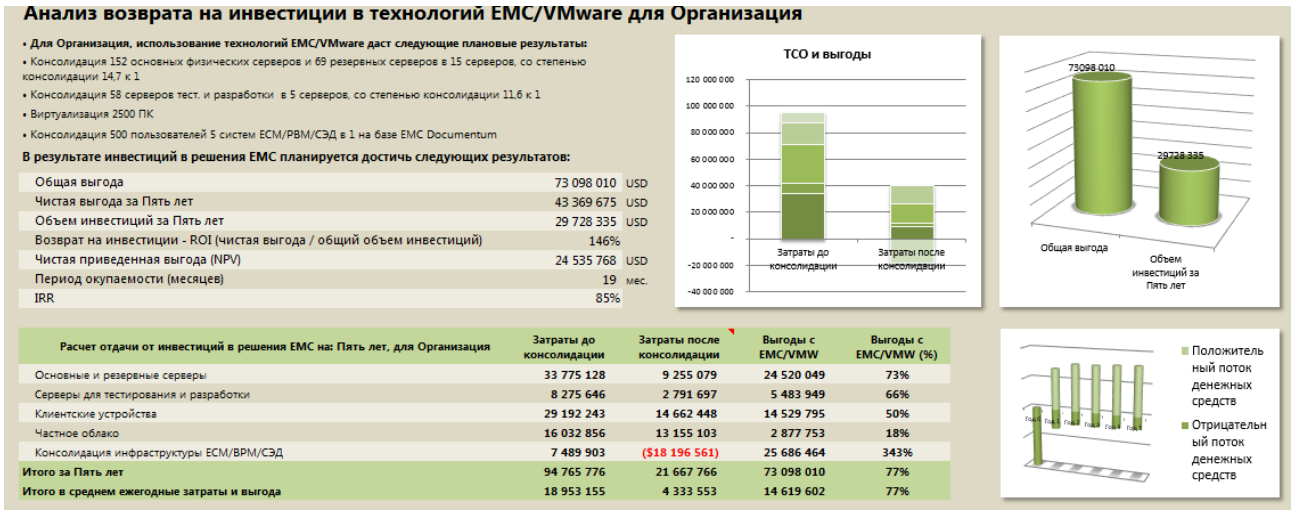
Используйте поля такого цвета для ввода исходных данных. Если вы не знаете значения соответствующего параметра, то для первоначального расчета можно использовать значения по умолчанию. Они, по возможности, соответствуют средним отраслевым и территориальным значениям.

Валюта для расчета	USD	Руб/USD	64
		EUR/USD	1,3
		Курс Валюта расчета/USD	1

Профиль организации

Название организации	Организация	
Какая отрасль наиболее близко соответствует основному виду деятельности? Для государственных организаций выберите "Правительство"	Высокие технологии и электроника	
В какой стране находятся основные центры по обработке данных?	Россия	
В каком регионе находятся основные центры по обработке данных?	Сибирский ФО	
Где находится основные центры обработки данных по отношению к центральной части городов?	Город	
Общее число пользователей ИТ, имеющих отношение к данному проекту?	2 500	
Общее число официальных рабочих часов в году	1981	
Доход (или бюджет) организации за прошлый финансовый год	1 000 000 000,00	USD
Валовая норма прибыли (профицит бюджета) организации за прошлый финансовый год	20%	
Учитывать рассрочку на 3 года / Software Assurance при расчете стоимости лицензий Microsoft?	Да	
Выберете из списка число лет, соответствующее необходимому периоду анализа ROI	Пять лет	
Ставка дисконтирования для учета временной стоимости денег	15,0%	
Средняя величина ежегодной поддержки используемого оборудования от закупочной цены, %	20%	

Рисунок 30 – Профиль организации



Анализ возврата на инвестиции в технологий EMC/VMware для Организация

- **Для Организация, использование технологий EMC/VMware даст следующие плановые результаты:**
- Консолидация 152 основных физических серверов и 69 резервных серверов в 15 серверов, со степенью консолидации 14,7 к 1
- Консолидация 58 серверов тест. и разработки в 5 серверов, со степенью консолидации 11,6 к 1
- Виртуализация 2500 ПК
- Консолидация 500 пользователей 5 систем ECM/PBM/СЭД в 1 на базе EMC Documentum

В результате инвестиций в решения EMC планируется достичь следующих результатов:

Общая выгода	73 098 010	USD
Чистая выгода за Пять лет	43 369 675	USD
Объем инвестиций за Пять лет	29 728 335	USD
Возврат на инвестиции - ROI (чистая выгода / общий объем инвестиций)	146%	
Чистая приведенная выгода (NPV)	24 535 768	USD
Период окупаемости (месяцев)	19	мес.
IRR	85%	

Расчет отдачи от инвестиций в решения EMC на: Пять лет, для Организация	Затраты до консолидации	Затраты после консолидации	Выгоды с EMC/VMW	Выгоды с EMC/VMW (%)
Основные и резервные серверы	33 775 128	9 255 079	24 520 049	73%
Серверы для тестирования и разработки	8 275 646	2 791 697	5 483 949	66%
Клиентские устройства	29 192 243	14 662 448	14 529 795	50%
Частное облако	16 032 856	13 155 103	2 877 753	18%
Консолидация инфраструктуры ECM/BPM/СЭД	7 489 903	($18 196 561)	25 686 464	343%
Итого за Пять лет	94 765 776	21 667 766	73 098 010	77%
Итого в среднем ежегодные затраты и выгода	18 953 155	4 333 553	14 619 602	77%

Рисунок 31 – Анализ ROI

Бюджет проекта (Отток ДС)	Год 0	Год 1	Год 2	Год 3	Год 4	Год 5
Затраты на ПО и оборудование	**- 6 923 543**	**- 3 852 214**	**- 4 124 629**	**- 4 400 739**	**- 4 440 468**	**- 4 736 591**
Затраты на лицензирование ПО и хранение данных для виртуализации основных серверов	924 285	1 319 599	1 505 410	1 647 129	1 556 492	1 698 025
Затраты на лицензирование ПО EMC и VMware для виртуализации лабораторных серверов	311 484	420 923	465 811	513 076	542 243	590 861
Затраты на лицензирование ПО, хосты, сети и хранение данных для виртуализации ПК	477 774	711 482	738 266	809 141	892 651	979 363
Затраты на лицензирование ПО для системы ECM (внутренний хостинг)	5 210 000	1 215 394	1 215 394	1 215 394	1 215 394	1 215 394
Затраты на новое оборудование для консолидированной системы ECM	-	184 816	199 749	215 999	233 687	252 948
Затраты на внедрение	**- 699 706**	**- 550 445**	**-**	**-**	**-**	**-**
Услуги подрядчиков по виртуализации основных серверов	131 250	-	-	-	-	-
Внутренние трудозатраты на внедрение виртуализации основных серверов	1 858	-	-	-	-	-
Затраты на обучение для внедрения основных серверов	4 000	-	-	-	-	-
Услуги подрядчиков по внедрению виртуализации серверов для разработки и тестирования	43 750	-	-	-	-	-
Внутренние трудозатраты на внедрение виртуализации серверов для разработки и тестирования	619	-	-	-	-	-
Затраты на обучение для внедрения виртуальных серверов для разработки и тестирования	-	-	-	-	-	-
Услуги подрядчиков для виртуализации ПК и приложений	212 500	-	-	-	-	-
Внутренние трудозатраты на внедрение для виртуализации ПК и приложений	10 083	-	-	-	-	-
Затраты на обучение для виртуализации ПК и приложений	6 000	-	-	-	-	-
Услуги подрядчиков по внедрению инфраструктуры частного облака	108 000	-	-	-	-	-
Внутренние трудозатраты на внедрение инфраструктуры частного облака	3 057	-	-	-	-	-
Затраты на обучение для внедрения инфраструктуры частного облака	-	-	-	-	-	-
Услуги подрядчиков по консолидации инфраструктуры ECM	171 000	-	-	-	-	-
Внутренние трудозатраты на внедрение инфраструктуры ECM	3 283	-	-	-	-	-
Затраты на обучение для внедрения инфраструктуры ECM	4 306	550 445	-	-	-	-
Итог:	**- 7 623 249**	**- 4 402 659**	**- 4 124 629**	**- 4 400 739**	**- 4 440 468**	**- 4 736 591**

Рисунок 32 – Инвестиции в проект

Приток ДС	Год 1	Год 2	Год 3	Год 4	Год 5
Выгоды от консолидации основной серверной инфраструктуры	**2 619 575**	**4 145 207**	**4 929 735**	**5 859 597**	**6 965 936**
Уменьшение числа основных серверов	622 990	867 597	905 928	945 670	986 845
Снижение затрат на покупку новых основных серверов	64 281	173 644	274 102	382 908	504 236
Снижение затрат на питание и охлаждение основных серверов	1 510 471	2 457 033	2 997 581	3 657 049	4 461 599
Уменьшение площади, занимаемой основными серверами	9 656	14 677	16 732	19 075	21 745
Снижение затрат на сетевую (LAN) инфраструктуру для основных серверов	52 200	74 400	81 600	91 200	100 800
Изменение затрат на хранение данных и сети хранения данных (SAN/СХД) для основных серверов	70 111	113 599	142 505	175 975	214 664
Снижение затрат на развертывание основных серверов	7 286	10 966	13 002	14 692	17 066
Снижение затрат на управление изменениями для основной серверной инфраструктуры	209 266	320 875	369 006	424 357	488 010
Снижение затрат на эксплуатацию основных серверов	65 715	100 763	115 878	133 260	153 249
Снижение затрат из-за плановых простоев (косвенная выгода)	3 151	4 833	5 558	6 391	7 350
Снижение затрат из-за неплановых простоев (косвенная выгода)	3 730	5 719	6 577	7 564	8 698
Уменьшение времени восстановления серверов в филиалах после аварий (косвенная выгода)	718	1 101	1 266	1 456	1 674
Уменьшение плановых простоев - рост доходов организации (косвенная выгода)	-	-	-	-	-
Уменьшение неплановых простоев - влияние на доходы (косвенная выгода)	-	-	-	-	-
Уменьшение времени восстановления после аварий - влияние на доходы (косвенная выгода)	-	-	-	-	-
Выгоды от консолидации серверной инфраструктуры для тестирования и разработки	**561 502**	**908 344**	**1 097 113**	**1 321 411**	**1 595 578**
Уменьшение числа серверов для тестирования и разработки	155 734	218 028	228 929	240 375	252 394
Снижение затрат на покупку новых серверов для тестирования и разработки	17 100	45 600	68 400	91 200	120 886
Снижение затрат на питание и охлаждение серверов для тестирования и разработки	454 259	738 928	901 492	1 099 820	1 341 781
Снижение затрат на площадь, занимаемую серверами тестирования и разработки	2 869	4 360	4 970	5 666	6 459
Снижение затрат на сетевую инфраструктуру (LAN) для серверов тестирования и разработки	14 400	19 200	21 600	21 600	24 000
Снижение затрат на сети хранения данных (СХД) и хранение данных для серверов разработки и тестирования	- 118 841	- 170 543	- 186 326	- 201 103	- 220 180
Снижение затрат на развертывание серверов для тестирования и разработки	17 779	26 075	28 683	31 551	34 706
Снижение затрат на воспроизведение ошибок в ПО	3 073	4 507	4 958	5 454	5 999
Снижение затрат на поддержку разрабатываемого ПО	14 058	20 618	22 679	24 947	27 442
Уменьшение времени на разработку, тестирование и выпуск внутренних приложений (косвенная выгода)	1 071	1 571	1 728	1 901	2 091
Уменьшение времени на разработку, тестирование и выпуск приложений для внешних клиентов (косвенная выгода)	-	-	-	-	-

Рисунок 33 – Выгоды от внедрения проекта

Выгоды от виртуализации клиентских устройств	2 250 308	3 118 328	2 635 129	3 028 436	3 497 594
Снижение затрат на обновление (замену) парка клиентских устройств	808 425	1 186 500	554 700	609 600	670 400
Снижение трудозатрат на обновление клиентских устройств	167 875	257 212	142 237	163 863	188 918
Снижение энергопотребления клиентскими устройствами	732 487	902 932	1 112 416	1 370 163	1 688 916
Снижение затрат на приобретение неиспользуемого ПО	24 375	35 750	39 325	43 257	47 583
Снижение затрат на управление настройками клиентских устройств	291 223	407 712	428 097	449 502	471 977
Снижение затрат на управление изменениями клиентской инфраструктуры	38 792	54 309	57 024	59 875	62 869
Снижение трудозатрат на обновления ОС	-	-	-	-	-
Снижение затрат на поддержку и администрирование клиентских устройств	97 646	136 704	143 540	150 717	158 253
Снижение затрат на поддержку различных видов и версий ОС	-	-	-	-	-
Снижение трудозатрат на обеспечение информационной безопасности клиентских устройств	2 076	3 183	3 661	4 210	4 842
Снижение трудозатрат на возобновление работы пользователей после аварий	3 566	5 468	6 288	7 231	8 316
Снижение трудозатрат на восстановление вышедших из строя клиентских устройств	3 883	5 953	6 846	7 873	9 054
Снижение рисков и затрат, вызванных потерями данных с клиентских устройств	47 250	72 450	83 317	95 815	110 187
Снижение затрат на поддержку пользователей клиентских устройств	14 928	22 889	26 322	30 270	34 810
Снижение операционных затрат пользователей на управление их конечными устройствами (косвенная выгода)	13 567	20 803	23 924	27 513	31 640
Снижение рисков информационной безопасности (косвенная выгода)	919	1 408	1 619	1 862	2 141
Снижение затрат на потерю работоспособности пользователей после аварий (косвенная выгода)	1 578	2 420	2 783	3 201	3 681
Снижение затрат на восстановление ПК после аварий (косвенная выгода)	1 718	2 635	3 030	3 484	4 007
Выгоды от перехода к частному облаку	**197 321**	**397 473**	**565 665**	**752 929**	**964 365**

Общая выгода	9 241 002	13 641 165	14 579 111	16 620 100	19 016 631	73 098 010

	Год 0	Год 1	Год 2	Год 3	Год 4	Год 5	
Отрицательный поток денежных средств	- 7 623 249	- 4 402 659	- 4 124 629	- 4 400 739	- 4 440 468	- 4 736 591	-29 728 335
Положительный поток денежных средств	-	9 241 002	13 641 165	14 579 111	16 620 100	19 016 631	73 098 010
Чистая выгода	- 7 623 249	4 838 342	9 516 536	10 178 372	12 179 633	14 280 040	43 369 675
Накопленная выгода	- 7 623 249	- 2 784 906	6 731 630	16 910 002	29 089 635	43 369 675	

Период окупаемости	
Период окупаемости для 3 или 4 лет, месяцев	Н/Д
Период окупаемости для 5 лет, месяцев	19

				Период анализа
	3 года	4 года	5 лет	Пять лет
NPV	10 472 319	17 436 064	24 535 768	24 535 768
Ставка дисконтирования	15%	15%	15%	

Рисунок 34 – Выгоды от внедрения проекта

Chargeback для основных серверных ВМ

	Хостов	CPU	Ядра	RAM	CPU, ГГц	Общее число основных ВМ
Основные хосты	15	60	240	1920	252	221
Из них резервные хосты	0	0	0	0	0	0
Итого ресурсов в ЦОД	**15**	**60**	**240**	**1920**	**252**	**221**
В среднем ресурсов на 1 ВМ	0,068	0,271	1,086	8,688	1,140	1,000

Типовой хост в кластере	Число	Резерв	Доступно	Переподписка (overcommit)	Доступно клиентам на хосте	Доступно клиентам в ЦОД
Число CPU	4	0%	4	0%	**4**	**60,00**
Число ядер	4	0%	4	0%	**4**	**60,00**
RAM (Гб)	128	0%	128,00	0%	**128**	**1920,00**
CPU (ГГц)	16,8	0%	16,8	0%	**16,80**	**252,00**

Хранение данных	Объем, Гб	Тип хранилища	Тип носителя	Стоимость покупки 1 Гб, в год	Число администраторов
Хранение основных серверных данны	22 100	SAN	Fiber Channel / RAID5	10	2
Данные резервного копирования основных серверов (backup)	22 100	SAN	iSCSI / RAID5	5	1
Хранение архивных данных	22 100	Ленточный накопитель	Магнитная лента	2	1
Итого	**66 300**			**USD**	**4**

Рисунок 35 – Себестоимость проекта

Статья затрат	Затраты за период	
Стоимость владения хостами	942 539	USD
Стоимость владения хранением данных и СХД	4 349 061	USD
Эксплуатационные затраты	1 542 739	USD
Затраты на лицензирование и внедрение системного ПО (базовый образ ВМ)	9 020 148	USD
Итого:	**15 854 487**	**USD**

Chargeback для вычислительных мощностей	% затрат на АО	Доступная мощность	Затраты за период за 1	Ежегодно	Ежемесячно	В час
			USD	USD	USD	USD
RAM (Гб)	50%	1920	245,45	49,09	4,09	0,006
CPU (ГГц)	50%	252	1 870,12	374,02	31,17	0,043

Chargeback для хранения данных	% затрат на АО	Доступная мощность	Затраты за период за 1Гб	Ежегодно	Ежемесячно	В час
			USD	USD	USD	USD
Хранение данных + СХД	100%	66 300	65,60	13,12	1,09	0,001

Chargeback для эксплуатационных затрат	% затрат на эксплуатацию	Затраты за период	Ежегодно	Ежемесячно	В час
		USD	USD	USD	USD
Эксплуатационные затраты	100%	1 542 739	308 547,80	25 712,32	35,20

Chargeback для затрат на внедрение	% затрат на внедрение	Затраты за период	Ежегодно	Ежемесячно	В час
		USD	USD	USD	USD
Затраты на лицензирование и внедрение системного ПО (базовый образ ВМ)	100%	9 020 148	1 804 029,64	150 335,80	205,80

Примеры конфигурации ВМ	Extra small VM (1GHz CPU, 768MB RAM)	Small VM (1.6GHz CPU, 1.75GB RAM)	Medium VM (2 x 1.6GHz CPU, 3.5GB RAM)	Large VM (4 x 1.6GHz CPU, 7GB RAM)	Extra large VM (8 x 1.6GHz CPU, 14GB RAM)	Средняя ВМ в ЦОД
RAM, Гб	0,750	1,75	3,5	7	14	8,69
CPU, ГГц	1	1,6	3,2	6,4	12,8	1,14
ХД, Гб	20	40	60	80	100	100,00
ХД резервное копирование, Гб	20	40	60	80	100	100,00
ХД архивная копия, Гб	20	40	60	80	100	100,00
Ежемесячно за вычислительные мощности	34,24	57,03	114,06	228,12	456,23	71,08
Ежемесячно за хранение данных и СХД	65,60	131,19	196,79	262,39	327,98	327,98
Ежемесячно эксплуатационные затраты на ВМ	116,35	116,35	116,35	116,35	116,35	116,35
Ежемесячно затраты на лицензирование и внедрение на ВМ	680,25	680,25	680,25	680,25	680,25	680,25
Итого, ежемесячно	**896,43**	**984,82**	**1 107,45**	**1 287,10**	**1 580,81**	**1 195,66**
	USD	USD	USD	USD	USD	USD
Итого, в год	10 757,18	11 817,84	13 289,35	15 445,20	18 969,74	14 347,95
Итого, в час	1,23	1,35	1,52	1,76	2,16	1,64

Рисунок 36 – Себестоимость проекта

На рисунках 30-36 представлен интерфейс данной модели.

Заключение

В результате написания магистерской диссертации достигнута основная цель – улучшение качества показателей инвестирования в облачные технологии. Для достижения данной цели разработана Консолидированная модель оценки эффективности использования виртуальных и облачных технологий. Модель разработана с учетом требования максимальной простоты в использовании и может быть использована неспециалистами в области информационной безопасности.

В рамках данной работы в соответствии с поставленными задачами, мною был проведен анализ деятельности текущего состояния облачных технологий с более детальным анализом предметной области – оценки эффективности внедрения облачных технологий, где были выявлены проблемы в организации данного процесса. Разработанная мною модель решает все эти проблемы.

Особое внимание было уделено выбору оптимального способа работы с экспертами. Установлено, что в данном случае оптимальным методом извлечения знаний является интервью, в основу которого положен один из методов экспертного оценивая – индивидуальный экспертный опрос.

Были проанализированы существующие пакеты программ для оценки инвестиционных проектов, на основании чего, был выбран инструментарий моделирования, предназначенный для оценки затрат и расчета экономической эффективности проектов консолидации систем управления контентом и оптимизации бизнес-процессов на базе технологий и решений EMC, VMware, Documentum.

В результате анализа существующих методик оценки рисков было принято решение о написании собственной модели оценки рисков на основании математического ожидания потерь.

Были выделены основные подсистемы для анализа, а так же риски, возникающие в данных подсистемах, и средства защиты по предотвращению возникновения рисков.

Был осуществлен подбор оптимальных технологий и средств разработки Консолидированной модели.

В ходе разработки данного ПО был спроектирован процесс выполнения операций, необходимых для выполнения основных задач при конвертации данных. Так же была спроектирована диаграмма сущностных классов, по которой в документациях интерфейса класса подробно расписаны назначение каждого класса и его функции.

Консолидированная модель оценки эффективности использования виртуальных и облачных технологий позволит проанализировать Индекс рентабельности инвестиций без учета оценки рисков, с учетом оценки рисков, а так же с учетом рисков и вложений в систему защиты.

В результате магистерской диссертации достигнута цель работы и выполнены все поставленные задачи. Дальнейшая работа над моделью предполагает расширение ее информационной базы, повышение эффективности алгоритмов оценки и совершенствование модели в целом.

Список используемых источников

1. Астахов, А. М. «Искусство управления информационными рисками» [Электронный ресурс]. – Режим доступа: http://анализ–риска.рф/content/cramm.

2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) / Федеральная служба по техническому и экспортному контролю, 2008 [Электронный ресурс]. – Режим доступа: http://fstec.ru/normativnye-i-metodicheskie-dokumenty-tzi/114-deyatelnost/tekushchaya.

3. Батура Т.В. Облачные технологии: основные понятия, задачи и тенденции развития [Текст]// Батура Т.В., Мурзин Ф.А., Семич Д.Ф. Программные продукты и системы и алгоритмы. – 2014. - №1. – С. 1-22.

4. Буриченко Т. Г. Анализ модели оценки эффективности использования облачных технологий [Текст]// Молодой ученый. – 2016. - № 1(3). – С. 252-260.

5. Буч Гради Язык UML [Текст]/ Гради Буч, Джеймс Рамбо, Ивар Якобсон – М.: ДМК-пресс, 2000.

6. Гиляровская Л.Т. Экономический анализ [Текст]/ Под. ред. Л. Т. Гиляровской. – М.: ЮНИТИ-ДАНА, 2006.

7. ГОСТ Р ИСО/МЭК 15408-1-2008 Критерии оценки безопасности информационных технологий: Введение и общая модель [Текст]. – М.: Изд–во стандартов, 2002. – 34 с.

8. Ефимова О.В. Финансовый анализ, Современный инструментарий для принятия экономических решений [Текст]/ О.В. Ефимова. – М.: Финансы и статистика, 2007.

9. Лешек А. Анализ требований и проектирование систем. Разработка информационных систем с использованием UML [Текст]/ Лешек А. Пер. с англ. – М.: Издательский дом «Вильямс», 2002. – 54 с.

10. Как оценить выгоду от переезда в облако [Электронный ресурс] – Хабрахабр – Режим доступа: http://habrahabr.ru/company/it-grad/blog/260515/.

11. Нечунаев, В. М. Оценка рисков информационной безопасности корпоративной информационной системы [Электронный ресурс]. – Режим доступа: http://www.tusur.ru/filearchive/reports-magazine/2009-1-2/51-53.pdf.

12. Облачные вычисления [Электронный ресурс] – Википедия – Режим доступа: https://ru.wikipedia.org/wiki/Облачные_вычисления.

13. Оценка эффективности от внедрения и использования методологии и инструментальных средств IBM Rational [Электронный ресурс] –IBM портал – Режим доступа: http://www.ibm.com/developerworks/ru/library/r-roi/.

14. Оценка эффективности IT-проектов [Электронный ресурс] – Дискуссионный клуб, открытый профессиональный портал – Режим доступа: http://dssclub.com.ua/categories/economics/.

15. Разумников С. В. Анализ существующих методов оценки эффективности информационных технологий для облачных IT- сервисов [Текст]// Современные проблемы науки и образования. – 2013. - № 3 – С. 37-33.

16. Разумников С. В. Оценка эффективности и рисков от внедрения облачных ИТ-сервисов [Текст]// Фундаментальные исследования. – 2014. - № 11.1 – С. 37-33.

17. Расчет ROI облачных сервисов [Электронный ресурс] – Содействие – Режим доступа: http://www.npsod.ru/blog/analytics/.

18. Савчук, В.П. Оценка эффективности инвестиционных проектов. Учебник [Текст]/В. П. Савчук. - М.: Перспектива, 2008. – 384 с.

19. Середенко Е. С. Оценка экономической эффективности аналитических информационных систем: дис. канд. Эконом. Наук. – М., 2014. – С. 18-29.

20. Скрипкин, К. Г. Эконом эффективность информационных систем. [Текст]/ К. Г. Скрипкин – М. : ДМК, 2012. – 115 с.

21. Современные методы и средства анализа и контроля рисков информационных систем компаний [Электронный ресурс] – iXBT – Режим доступа: http://www.ixbt.com/cm/informationsystem-risks012004.shtml.

22. Федеральный государственный образовательный стандарт высшего образования (ФГОС ВО) по направлению подготовки «Прикладная информатика» (уровень магистратуры), утвержденный приказом Министерства образования и науки Российской Федерации от 30 октября 2014 г. №1404.

23. Угрозы безопасности в облаке [Электронный ресурс] – TAdviser Режим доступа: http://www.tadviser.ru/index.phpindex.php/ Статья:Главные_угрозы_безопасности_в_облаке.

24. Управление бизнес-процессами. Среда разработки в BPWin. [Электронный ресурс] – Электронные данные – Режим доступа: http://www.interface.ru/home.asp?artId=2736.

25. Управление бизнес-процессами. Среда разработки в StarUML. [Электронный ресурс] – Электронные данные – Режим доступа: http://ru.winportal.com/staruml.

26. Forrester works with business and technology leaders to develop customer-obsessed strategies that drive growth [Электронный ресурс] – Forrester – Режим доступа: https://www.forrester.com/home/.

27. 2015 StateoftheCloudReport [Электронный ресурс] – Отчет использования облака 2015 – Режим доступа: http://www.rightscale.com/.

28. Елиферов, В.Г. Бизнес-процессы: Регламентация и управление: Учебник [Текст]/ В.Г. Елиферов. – М.: НИЦ ИНФРА-М, 2013. – 319 с.

29. Репин, В.В. Бизнес-процессы. Моделирование, внедрение, управление [Текст]/ В.В. Репин. – М.: Манн, Иванов и Фербер, 2013. – 512 с.

30. Крышкин, О. Настольная книга по внутреннему аудиту: Риски и бизнес-процессы. 3 – е изд. [Текст]/ О. Крышкин. – М.: Альпина Паблишер, 2016. 477 с.

31. Ротер, М. Учитесь видеть бизнес-процессы: Построение карт потоков создания ценности. 4 – е изд. [Текст]/ М. Ротер. – М.: Альпина Паблишер, 2015. 136 с.

32. Тельнов, Ю.Ф. Инжиниринг предприятия и управление бизнес-процессами. Методология и технология: Учебное пособие [Текст]/ Ю.Ф. Тельнов, И.Г. Фёдоров. – М.: ЮНИТИ, 2015. – 176 с.

33. Чукарин, А.В. Бизнес – процессы и информационные технологии в управлении современной инфокоммуникационной компанией [Текст]/ А.В. Чукарин. – М.: Альпина Паблишер, 2016. – 512 с.

34. Репин, В.В. Процессный подход к управлению. Моделирование бизнес – процессов [Текст]/ В.В. Репин. – М.: Манн, Иванов и Фербер, 2013. – 544 с.

35. Громов, А.И. Управление бизнес-процессами: современные методы монография [Текст]/ А.И. Громов, А. Фляйшман, В. Шмидт. – Люберцы: Юрайт, 2016. – 367 с.

36. Ширяев, В.И. Управление бизнес-процессами: Учебно – методическое пособие [Текст]/ В.И. Ширяев, Е.В. Ширяев. – М.: Финансы и статистика, 2014, 464 с.

37. Джестон, Д. Управление бизнес-процессами. Практическое руководство по успешной реализации проектов [Текст]/ Д. Джестон, Й. Нелис. – М.: Символ, 2015. – 512 с.

38. Долганова, О.И. Моделирование бизнес-процессов: Учебник и практикум для академического бакалавриата [Текст]/ О.И. Долганова, Е.В. Виноградова, А.М. Лобанова. – Люберцы: Юрайт, 2016. – 289 с.

39. Михеев, А.Г. Системы управления бизнес-процессами и административными регламентами на примере свободной программы RunaWFE. [Текст]/ А.Г. Михеев. – М.: ДМК, 2016. – 336 с.

40. Клементьев И. П. Введение в облачные вычисления. [Текст]/Клементьев И. П. Устинов В. А. – УГУ, 2009

41. Нил Склейтер. Облачные вычисления в образовании: Аналитическая записка [Текст]/ Пер. с англ. Институт ЮНЕСКО по информационным технологиям в образовании. - Москва, 2010

42. Облачные сервисы: взгляд из России [Текст]/ под ред. Е. Гребнева. – М.: Cnews, 2011

43. Широкова Е. А. Облачные технологии. [Текст] - Уфа: Лето, 2011

44. Исаев Е.А., Корнилов В.В., Тарасов П.А. Научные компьютерные сети – проблемы и успехи в организации обмена большими объемами научных данных. Математическая биология и биоинформатика [Электронный ресурс]. 2013. Т. 8. № 1. С. 161–181. URL: http://www.matbio.org/2013/Isaev_8_161.pdf.

45. Hoff Ch., Simmonds P. Security guidance for critical areas of focus in cloud computing. Website of Cloud Security Alliance [Электронный ресурс]. 2011. С. 12–20. URL: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

46. Khajeh-Hosseini A., Sommerville I., Sriram I. Research Challenges for Enterprise Cloud Computing. arXiv.org: Cornell University Library [Электронный ресурс]. URL: http://arxiv.org/ftp/arxiv/papers/1001/1001.3257.pdf.

47. An overview on cloud computing for research and science published [Электронный ресурс]. 2012. URL: http://www.e-irg.eu/news/news/479/an-overview-on-cloud-computing-for-research-andscience-published.html.

48. Розенблюм М., Гарфинкель Т. Мониторы виртуальных машин: современность и тенденции. Открытые системы [Электронный ресурс]. 2005. № 05–06. URL: http://www.osp.ru/os/2005/05-06/185589/

49. Федоров А.Г. Облачная платформа Microsoft. 2010. [Текст]/ Федоров А.Г., Мартынов Д.Н. - 100 с.

50. Stiefel M. Cloud Computing with Microsoft Azure. Website of Reliable Software [Электронный ресурс], Inc. 2009. URL: http://reliablesoftware.com/presentations/Introduction%20to%20Cloud%20Computing %20with%20Microsoft%20Azure.pdf.